事故事例分析に基づく情報システム開発のリスク対策方法

論文（査読論文）

事故事例分析に基づく情報システム開発のリスク対策方法

A Risk Management Method for Information System Developments Based on Accident Case Analyses

齋田芽久美 Megumi SAIDA
平林元明 Motoaki HIRABAYASHI
湯浦克彦 Katsuhiko YUURA
静岡大学大学院情報学研究科

要旨：
情報システム開発における要件定義に欠陥があると，システムの品質・コスト・納期に大きな影響を与えてしまう．要件定義に必要な技術知識を提供するものとしてTRM(Technical Reference Model) などがあるが，経験の少ない担当者にとっては学ぶべき範囲が広く，要件定義記述に生かしにくかった．
本研究では専門雑誌における情報システムに関連する事故の事例記事を収集し，事故の要因ごとに分類し，要因に基づく事故の傾向や，要因と要件項目の関係を分析した．また要件項目ごとに，これらの関係情報を参照できる要件定義支援環境の提案を行った．これらの成果に関して省庁のCIO 補佐官など要件定義の専門家のレビューを受け，要件定義担当者の育成に効果が期待できるという評価を得た．

キーワード：情報システム，事故要因，要件定義

Abstract：
When request definitions of information system development have defects, qualities, costs and delivery time of the system become significantly degraded. TRM(Technical Reference Model) shows technical knowledges for request definition, but it is not so easy to understand for less experienced engineers.
In this paper, accident case articles of information system are collected, accident factors are analyzed and classified, and trends of the factors and relations among the accident factors, request definition items and the technical knowledges are analyzed. A request definition assistant environment to search the factors, the knowledges, the relations and so on is designed. Professionals of request definition including CIOs evaluate that the features of the assistant environment are useful for training of young engineers.

keywords: Information System, Accident Factor, Request Definition

1. はじめに

情報システム開発においては，実際にプログラミングやテストなどの作業を通してシステムを開発する下流工程に先立ち，情報システムの開発によって業務上のどういう課題をどのように解決していくかを明確にする上流工程が重要な工程として設けられる．上流工程は，一般に解決したい課題を認識する計画フェーズと，どのように関係するかを具体化する要件定義フェーズに分けられる．要件定義フェーズでは業務上の課題を解決する機能に関する機能要件だけではなく，どれくらいの性能・品質で業務上の課題を解決するのかという非機能要件も定義する．

要件定義の欠陥は，いずれもその修正が後

になればなるほど必要なコストが増加し，情報システム構築における品質・コスト・納期に大きな影響を与えることになる．にも関わらず，我が国における情報システム開発においては十分な体制が整備されずに問題を生じさせていることが少なくない．たとえば政府調達の情報システムに関して，2007 年に府省情報化統括責任者 (CIO) 連絡会議で決定された「情報システムに係る政府調達の基本方針」[1] の第一章においては，下記のように述べられている．

> 「情報システムに係る政府調達においては，競争環境が適切に確保されていないのではないかといった調達手続上の課題，調達工程の進ちょく管理や調達成果物の品質管理が適切に行えていないのではないか，情報システムに係る経費が割高となっており適切な費用対効果が得られていないのではないかといった調達管理上の課題等，従来からの課題が未だに解決されていない状況にある．」

要件定義の作業を円滑に進めるには，当該業務に関する知識のほか，次々と刷新されていく情報システム技術に関する広範な知識が必要となる．この技術知識の獲得を支援するものの一つとして，経済産業省および IPA(Information-technology Promotion Agency，独立行政法人 情報処理推進機構) から「情報システム調達のための技術参照モデル (TRM:Technology Reference Model) の物品調達編 [2] および役務調達編 [3] が公開されている．また，情報システムの品質に関わる知識を支援するものとして，IPA から非機能要求グレード [4] が公開されている．要件定義の担当者は，必要に応じてこれらの資料を参照することができるようになった．

しかし，これらの資料は情報システム技術のすべてを網羅した大規模なものであり，要件定義の担当者，特に経験の少ない多くの要件定義担当者にとって親しみにくいものとなっている．これらの知識を要件定義書の作成に活用するためには，要件項目がそれぞれどのようなトラブルに繋がりやすいのか，またそのトラブルを防ぐためにはどのように要件を定義したら良いのかを理解し，資料の調査範囲を絞って利用することが必要と考えられる．

本研究では，実際に起こった情報システム関連事故の紹介記事を分析し，事故の動向と要因の関係を分析し，重要視すべき事故事例や事故要因を明らかにする．また TRM や非機能要求グレードなど標準化を指向した知識体系に対応付けて，事故の要因項目と要件定義の項目の関係を明らかにする．これらの関係に基づいて，経験の少ない要件定義担当者が要件項目の重要性と特徴を理解することができる要件定義支援環境を提案することを目的とする．

本論文では，まず情報システム開発の工程，要件，要件定義のための知識などに関する既存の体系と関連研究について述べる（第 2 節）．そのうえで，実際に起こった情報システム関連事故の紹介記事を収集して要因ごとに整理し，各要因と事故の生起頻度や動向，各要因と要件定義項目との関係などを分析する（第 3 節）．その結果を活用して，要件項目の重要性と特徴を理解しながら要件定義書を作成していく支援環境を提案する（第 4 節）．さらに，情報システムの事故要因に関する考察と，要件定義支援環境の提案に対する専門家の評価をまとめる（第 5 節）．最後に，結論と今後の機能拡大についての展望を述べる（第 6 節）．

2. 要件定義書作成を支援する従来の方法

2.1 情報システム開発における要件定義の位置付けと重要性

情報システム開発に流れと要件定義の位置付けについて述べる，情報システム開発の流れについては ISO/IEC12207:2008 ソフトウェアライフサイクルプロセスを国内向けに拡張した共通フレーム 2013[5] あるいは ISO/IEC15288:2008

図 2_1. 情報システム開発の流れと要件定義の位置付け

システムライフサイクルプロセス [6] などが標準モデルとして知られているが，本研究では，おもに政府調達システムを対象としていくので，総務省から提供されている情報システムに係る政府調達の基本指針 [7] に基づいて説明する．

情報システム開発は大きく，情報システム化計画の策定，要件定義，設計･開発，テスト，運用保守のフェーズに分かれる．情報システム化計画の策定では，現行の業務とシステムの分析を行って現状を明らかにし，現状の問題点を整理する．現状の問題点について情報システムを用いて解決する場合，次の要件定義フェーズでは情報システムに必要な機能, 品質を定義し，要件定義仕様書を作成する．その後設計フェーズでは要件定義仕様書を元にシステムのイメージをより具体的にし, 開発とテストを繰り返す．総合テスト完了後に開発環境から実稼働環境へと移行，新業務の運用開始となる．情報システム化計画のフェーズから要件定義のフェーズまでを一般的に上流工程と称し，この上流工程でプロジェクトの方向性は決定されることになる．高度な幅広い技術知識と業務知識が必要とされる責任度と難易度の高いフェーズである．

2.2 情要件定義の概要

要件定義の概要について，総務省による「情報システムに係る政府調達の基本指針」[7] を参考に説明する．

要件定義書は，大きく分類して３つの要素で構成されている．１つは業務要件で，現行の業務や新しい業務のあり方をフロー図などで検討し，入出力する情報などを定義する．あとの２つはシステムに関わる要件であり，機能要件と非機能要件に分けることができる．機能要件はシステムで新しい業務を実現するために実装する機能を定義し，非機能要件はシステムの品質に関して，規模･性能，セキュリティ，移行，運用・保守などについて定義したものである．業務要件では，情報システム導入の目的，読み手によって複数の解釈が可能な専門用語などの意味，情報システムに係る業務の全体像，情報システム化の範囲，納入すべき成果物とそのスケジュールなどを記述する．機能要件では，システム化する機能・画面・帳票の一覧とその概要，構築する情報システムで取り扱う情報やデータに関することを記述する．非機能要件で

表 2_1. 要件定義項目 [7]

調達仕様書
表紙 ・調達件名
作業の概要 ・目的　・情報システム化の範囲 ・用語の定義　・作業内容・納入成果物 ・業務の概要
機能要件 ・情報システムの要件（機能、画面、帳票、情報・データ、外部インタフェース）
非機能要件 ・規模・性能要件 ・信頼性要件（信頼性、拡張性、上位互換性、システム中立性、事業継続性） ・情報セキュリティ要件（権限、情報セキュリティ対策） ・システム稼働環境（全体構成、ハードウェア構成、ソフトウェア構成、ネットワーク環境、アクセシビリティ） ・テスト要件 ・移行要件（移行、教育） ・運用要件（情報システムの操作・監視等、データ管理、運用施設・設備） ・保守要件（ソフトウェア保守、ハードウェア保守） ・作業の体制及び方法（作業体制、開発方法、導入、瑕疵担保責任） ・特記事項
業務・システム最適化計画等の関係書類

は，構築する情報システムの規模・性能要件，信頼性要件 (拡張性, 上位互換性, 可用性など), セキュリティ要件，テスト・移行・運用・保守要件，作業体制などを記述する．

2.3 システム管理基準

システム管理基準 [9] は，情報戦略を立案し効果的な情報システム投資やリスク管理を行うための事項を取りまとめたものであり，2004 年に経済産業省から公開されている．システム

表 2_2. システム管理基準の項目 [9]

大項目	中項目
Ⅰ情報戦略	1.全体最適化
	2.組織体制
	3.情報化投資
	4.情報資産管理方針
	5.事業継続計画
	6.コンプライアンス
Ⅱ企画業務	1.開発計画
	2.分析
	3.調達
Ⅲ開発業務	1.開発手順
	2.システム設計
	3.プログラム設計
	4.プログラミング
	5.システムテスト・ユーザ受入れテスト
	6.移行
Ⅳ運用業務	1.運用管理ルール
	2.運用管理
	3.入力管理
	4.データ管理
	5.出力管理
	6.ソフトウェア管理
	7.ハードウェア管理
	8.ネットワーク管理
	9.構成管理
	10.建物・関連設備管理
Ⅴ保守業務	1.保守手順
	2.保守計画
	3.保守の実施
	4.保守の確認
	5.移行
	6.情報システムの廃棄
Ⅵ共通業務	1.ドキュメント管理
	2.進捗管理
	3.品質管理
	4.人的資源管理
	5.委託・受託
	6.変更管理
	7.災害対策

ライフサイクルを企画・開発・運用・保守の４つの業務に定義した上で６つの大項目から構成されている．（表 2_2）

Ⅰ . 情報戦略では，全体最適化の方針，目標を明確にして策定することなどが挙げられている．Ⅱ . 企画業務では，ユーザニーズや現状分析を適切に行い，開発計画を立てることなどが記述されている．Ⅲ . 開発業務では，設計の際に考慮すべきこと，システムテスト・ユーザ受入れテスト，移行時に気をつけるべきことが記述されている．Ⅳ . 運用業務では, 運用管理ルールの策定，遵守などが記述されている．Ⅴ . 保守業務では，保守手順の策定，計画，実施，実施後の確認方法や移行方法などについて記述されている．Ⅵ . 共通業務では，ドキュメント，進捗，品質，人的資源の管理や委託業務について，バックアップ方法，代替処理や復旧について記述されている．

各項目は中項目，さらに小項目にまで分かれており，287 項目が記載されている．

2.4 情報セキュリティ管理基準

情報セキュリティ管理基準 [10] は，組織体が効果的な情報セキュリティマネジメント体制を構築し，適切なコントロール・運用するための実践的な規範として策定されたものであり，経済産業省から提供されている．初版は 2003 年に策定されたが，その後情報セキュリティマネジメントに関わる重要な国際規格が策定されるという国際規格化の動きを受け，国際規格との整合を取るために見直しを行い，2008 年には情報セキュリティ管理基準（平成 20 年改正版）へと版を改訂している．

情報セキュリティ管理基準（平成 20 年度改正版）はマネジメント基準と管理策基準から構成されている．マネジメント基準では情報セキュリティマネジメントの計画，実行，点検，処置に必要な実施項目を定めている．管理策基準は組織の情報セキュリティマネジメントの確立段階においてリスク対応方針に従って管理策

を選択する際の選択肢を与えるものである．本研究では，主に管理策基準を参照する．管理基準は 11 の大項目と 39 の中項目で構成されている．（表 2_3）

表 2_3. 情報セキュリティ管理基準の大項目 [10]

項目番号	項目
1	セキュリティ基本方針
2	情報セキュリティのための組織
3	資産の管理
4	人的資源のセキュリティ
5	物理的及び環境的セキュリティ
6	通信及び運用管理
7	アクセス制御
8	情報システムの取得、開発及び保守
9	情報セキュリティインシデントの管理
10	事業継続管理
11	順守

1. セキュリティ基本方針では，情報セキュリティの基本方針とその文書について記述されており，2. 情報セキュリティのための組織では，組織内の情報セキュリティの管理，外部組織によって管理されている情報及び施設のセキュリティを維持することについて記述されている．3. 資産の管理では，組織の資産を適切に保護し維持するための資産に対する責任などについて記述している．4. 人的資源のセキュリティでは，従業員，契約相手及び第三者の利用者がその責任を理解し，盗難，不正行為のリスクを低減することなどが記述されている．5 物理的及び環境的セキュリティでは，組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止することなどが記述されている．6. 通信及び運用管理では，悪意あるコードからの保護やネットワークにおける情報の保護などが記述されている．7. アクセス制御では，情報へのアクセスを利用者やグループごとに制御すること，パスワード選択及び利用時に正しいセキュリティ慣行の順守を利用者に要求することなどが記述されている．8. 情報システムの取得，開発及び保守では，情報漏洩の可能性を抑止することと，技術的脆弱性の管理について記述されている．9. 情報セキュリティインシデントの管理では，情報システムに関連する情報セキュリティの事象及び弱点を適切な管理者への連絡経路を通して，できるだけ速やかに報告することなどが記述されている．10. 事業継続管理では，情報システムの重大な故障または災害の影響から重要な業務を保護し，また事業活動及び重要な業務の時期を逃さない再開を確実にすることなどが記述されている．11. 順守では，法的要求事項の順守，組織のセキュリティ方針への順守，情報システムの監査に対する考慮事項などについて記述されている．

2.5 TRM

2.5.1 EA と TRM

調達仕様書作成における技術知識や業務知識の不足を補うために，経済産業省と IPA により調達仕様書作成段階で必要となる技術知識をまとめた TRM が公開されている．

TRM は EA(Enterprise Architecture) における参照モデルの 1 種である [11]．EA とは企業における業務・システムの最適化の方法論であり，企業や組織において個々のシステムの開発に先だってその企業・組織に共通なアーキテクチャを設計することを主旨としている．企業・組織においてこのアーキテクチャを設計するための参照モデルの一つとして TRM は設けられている．EA には TRM の他に PRM(Performance Reference Model)，BRM(Business Reference Model)，SRM(Service Component Reference Model)，DRM(Data Reference Model) の 4 つの参照モデルが存在し，それぞれシステムの価値評価指標，ビジネス，アプリケーション・サービス，データの共通的な知識が記載される (図 2_2)

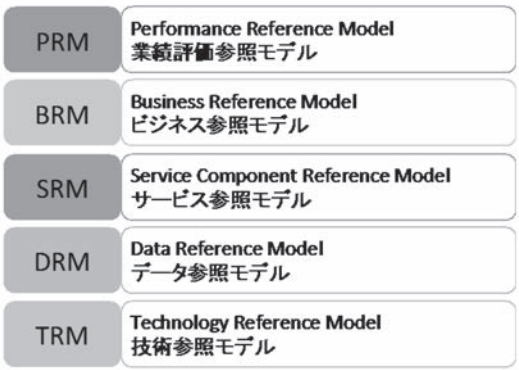


図 2_2. EA(米国 V1.1 および経済産業省版) における 5 つの参照モデル

2.5.2 TRM「物品調達編」

TRM 物品調達編では，様々な機能・サービスを 18 の技術ドメインに分け，それぞれを解説している．表 2_4 は TRM 物品調達編の目次である．

「2. 技術ドメイン解説」の内容について，「2.1 BI/DWH/ETL」を例に紹介する．

「2.1 BI/DWH/ETL」は意思決定をより素早く適切に行うために，ユーザに対して適切な情報を提供するシステムの総称であり，このドメインには BI，DWH，ETL，データマート，OLAP，ODS，データマイニング，ダッシュボード，レポーティングツール，スプレッドシートという機能・サービスが含まれている．それぞれの機能・サービスにはその定義の説明，基本要素，加点要素・選択要件としての要件の内容と関連技術が記載されている．

表 2_4. TRM 物品調達編目次 [2]

目次	
1.まえがき	1.1概要
	1.2文書の構成
2.技術ドメイン解説	2.1BI/DEH/ETL
	2.2EAI
	2.3iDC・設備
	2.4SOA関連機能
	2.5保守環境
	2.6サーバ
	2.7ストレージ
	2.8共通PC・オフィスプリンタ
	2.9運用管理
	2.10EIP
	2.11公開Webサーバ
	2.12グループウェア、ファイルサーバ、メールサーバ
	2.13統合アカウント管理・認証・認可（アクセス制御）
	2.14統合ディレクトリ
	2.15WAN、省内LAN、DNS/DHCP/Proxy、リモートアクセス
	2.16ワークフロー、BAM
	2.17セキュリティ
	2.18ドメイン共通

2.5.3 TRM「役務調達編」

TRM 役務調達編では，情報システム調達において調達すべき「役務」，すなわちやるべき作業の仕様書への記載方法を解説している．

図 2_3 は TRM における役務を情報システム

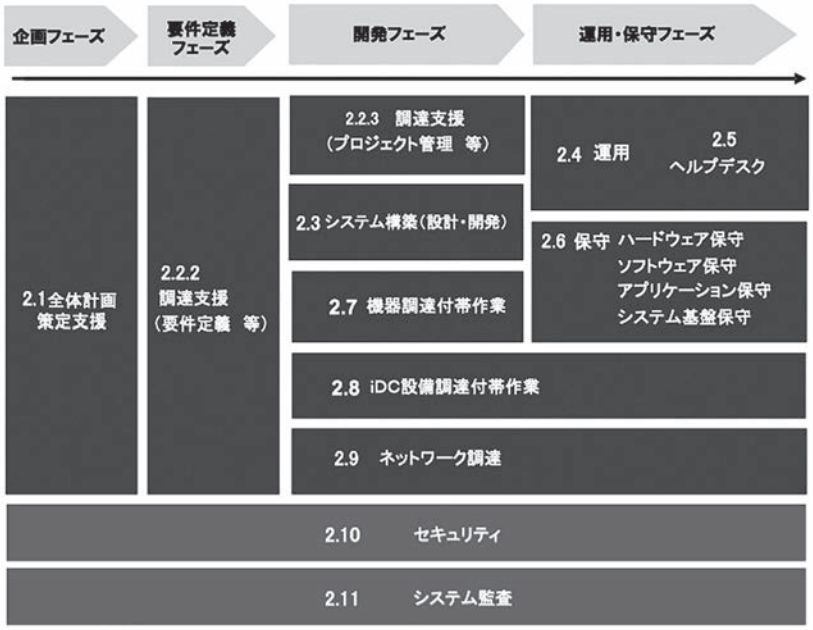


図 2_3. TRM における役務一覧 [3]

の４つのフェーズ，「企画フェーズ」「要件定義フェーズ」「開発フェーズ」「運用・保守フェーズ」で分類した図である．TRM における役務は 10 の役務で構成されており，たとえば，企画フェーズには「2.1 全体計画策定支援」，要件定義フェーズには「2.2.2 調達支援（要件定義等）」が含まれる．「2.2.2 調達支援（要件定義 等）」などの項には，役務の概要，発注者側で用意しておくべきもの，この役務で作成される成果物，仕様書に記載すべきポイントや記載の例，案件・情報システムの特性等による留意点，セキュリティに関する留意点等の情報が書かれている．

2.6 非機能要求グレード

非機能要求グレードは情報システム開発の非機能要求について，発注者と受注者との認識の行き違いなどを防止することを目的として IPA から提供されている非機能要求の確認を行うツール群である．

非機能要求グレードはシステム基盤に関わる非機能要求を対象としており，要求を可用性，性能・拡張性，運用・保守性，移行性，セキュリティ，システム環境・エコロジーの６つの大項目に整理している．（表 2_5）

非機能要求グレードにはグレードという概念が導入されている．情報システムは利用目的，規模，性質や特徴に多様性があるために，すべてに対して非機能要求を一意に定めることができない．そのため，各非機能要求の項目に 0 ～ 5 のレベル値と対応する条件が設定されている．また，情報システムを社会的影響の有無などにより３つに分類したモデルシステムを定義し，それぞれに対して各非機能要求の項目のレベル値を設定している．

2.7 関連研究

2.7.1 情報システム開発のリスクマネジメント全般に関する研究

IPA のソフトウェア・エンジニアリング・センターでは，重要インフラ情報システム信頼性研究会を設置し，鉄道，航空，金融，物流など国民生活や社会経済活動にとって重要な社会サービスと，その社会サービスを提供する情報システムの信頼性について研究し成果 [15] を公表している．情報システム開発に関わる経営層，事業部門，情報システム部門，IT ベンダーのそれぞれの役割に基づく開発・運用の管理フレームワークが提唱されるとともに，国内における実施例が紹介されている．本研究においても，こうしたユーザ企業・IT 企業の両者にわたる役割分担に言及する部分もあるが，要件定義の担当者による要件定義書（調達仕様書）記述の作業に焦点を絞り，事故の要因項目と要件定義の項目との関係を示して記述を支援する方法を具体化している．

遠藤ら [16] による金融に関わる情報システムのリスクマネジメントの研究では，金融事業者のリスクと金融情報システムのリスクを対比し，過去のシステム障害事例に立脚しつつ，システム開発の成功要因に不可欠な 6 つの要件（A．経営トップのコミットメント確立，B．組織体制と IT ガバナンス，C．IT リスクの適切な評価と対策の構築，D．拡張性一貫性の確保，E．非機能要件を含む要件定義最適化，E．品

表 2_5. 非機能要求グレード大項目

大項目	特徴的な非機能要求
可用性	稼働率、目標復旧水準、大規模災害
性能・拡張性	性能目標、拡張性
運用・保守性	運用時間、バックアップ、運用監視、マニュアル、メンテナンス
移行性	移行方式の規定、移行スケジュール、設備・データ
セキュリティ	重要資産の公開範囲
システム環境・エコロジー	制限、耐震

質重視の仕組み構築）を提言している．本研究と同じく情報システムの事故につながる要因を分析しているが，その要因は本研究のようにおもに要件定義フェーズにおける要件定義担当者の作業に視点を置くものではなく，おもに経営トップの情報システムへの関わり方や組織全体の体制・システム業務分担のあり方などに視点を置いて分析している．そこで，経営者や組織の運営に当たる管理者の役割に関わる要因に関しては遠藤らの研究がより詳しいが，上記の 6 つの要件のうちの特に要件定義に関連の深い C, E, F において，本研究がより詳細な分析と対策の立案となっている．

宮坂ら [17] は，企業統合に伴って発生する全社的な IT システム統合に注目し，そこで必要とされるリーダーシップについて，国内の大手金融機関における成功事例と失敗事例を比較している．特に経営トップの行動がプログラムマネージャーである CIO(Chief Information Officer) へ与える影響について分析している．西尾 [18] は，銀行のシステム統合の事例分析をもとに，情報システム開発のリスクマネジメントに関して CIO が担うべき役割について述べている．本研究では，経営者や CIO の役割ではなく，CIO によって管理される要件定義の担当者の行動の支援方法を述べている．

2.7.2 情報システムの事故事例分析に関する研究

坂東ら [19,20] は，通信ネットワークおよび金融情報システムに関する全国紙 4 紙の報道記事を収集し，事故の傾向，重大性や原因に関する分析をおこなった．事故原因については，開発フォールト（設計ミスなど），物理的フォールト（部品劣化など内部要因／自然災害など外部要因）および人為的フォールト（悪意なし／悪意あり）に分類している．本研究も同様にメディアに記載された情報から事故の傾向，重大性と原因を分析しているが，雑誌の豊富な記述を利して，事故の原因を分析し，それを生んだ情報システム開発プロセスや要件定義上での留意点と関係付けている．これにより，要件定義を行う際の参考情報として提供し，事故の低減に役立てようとしたころに特徴がある．

日本銀行では，国内の金融機関からの報告や，金融機関に対する考査・オフサイトモニタリングによって収集した金融情報システムの障害情報を分析している [21]．障害はハードウェアに起因した障害，ソフトウェアに起因した障害，システム性能に起因した障害および運用・保守に起因した障害の 4 種に大別され，システムリスク管理の体制・プロセス，システム開発管理，情報セキュリティ管理，システム障害管理の 5 種類からなる対応策が提言されている．障害事例と原因・対策の情報を開発関係者に対して提供するという点において本研究と同様であるが，本研究では，システム管理基準，情報セキュリティ基準や TRM など標準化された情報システム開発体系に基づいて事故原因を分析しているため，これらの体系に即した要件定義書の各パートに直接対応付けて参考となる情報の提供が可能となっていることが特徴である．

2.7.3 要件定義の品質向上に関する研究

青山ら [22] は，システムの要求定義に関する知識体系である REBOK を提案している．ソフトウェア工学の観点から，技術者が顧客から要求を引出し，それを分析し仕様として定義していく過程やそこで必要とされる技術や知識を共有する枠組みを示している．本研究は，REBOK で定義している８つの知識領域のうちの「実践上の考慮点」あるいは「要求分析」に該当する知識の一つあるいは知識の提供法の一つとして具体化したものと位置付けることが可能である．本研究で狙いとする事故事例情報の提供は「実践上の考慮点」に含むと考えられ，事故事例情報を参照して要件項目を検討する方法は「要求分析」に含むと考えられる．

齊藤ら [23] は，ベンダーへの提案依頼書 (RFP: Request for Proposal) の記述の品質を定量的に評

価する方法を提案している．RFP は要件定義書とほぼ同様の内容を持つと考えられる資料である．この研究では評価対象とする要件定義項目を，情報システム開発において特に重要度の高い「保守と運用に関する 55 の非機能要件」のみに定め，その記述の明確さを評価する方法を示している．本研究と同じく要件定義を支援することを目的とするが，本研究では事故事例情報に基づいて，特に注意すべき要件項目を提示するのに対し，この研究では要件項目全体にわたって記述の品質を高めるというアプローチの違いがある．また，齊藤らの研究ではユーザが行った要件定義をユーザ自身が評価する時点のみを支援するが，本研究ではユーザが情報システムの要件定義を記述する時点も支援することができる．

佐藤ら [24] は，標準化された品質特性 (ISO9126[25]) とそれに関連深いキーワードとの対応表を用意し，要求仕様書のテキストにそれらのキーワードがどのくらい出現するかを分析することによって，その要求仕様の品質要求含有率を計測するツールを開発した．この研究も要件定義を評価する時点を支援するだけで，要件定義を記述する時点を支援する機能は有しない．

3. 情報システムに関わる事故事例の要因分析

3.1 事故事例の要因分析手順

3.1.1 事故事例

本研究では社会的に問題となった事故事例を分析するため，日経 BP 社が発刊している雑誌「日経コンピュータ」の記事の 1 つである「動かないコンピュータ」[8] において掲載されている事故事例の紹介記事を収集した．「動かないコンピュータ」では社会的に大きな問題となった情報システム開発の事故における，ユーザ企業やベンダー，コンサルティング会社の責任について数多く取り上げており，1981 年 10 月の創刊から 1997 年 4 月まで連載されていた．その後「動かないコンピュータ」は「誤算の検証」と名称を変えて 2001 年 1 月 1 日から再開し 2001 年 9 月 24 日まで連載，2001 年 10 月 22 日から 2005 年 5 月 30 日までは「誤算の検証 動かないコンピュータ」と名称を変え，さらに 2005 年 6 月 13 日から 2015 年 9 月現在も引き続き「動かないコンピュータ」という名称で「日経コンピュータ」に記事が掲載されている．

3.1.2 分析手順

本研究ではまず，2001 年 1 月 1 日から 2014 年 9 月 24 日までに発行されている 332 件の事故事例記事を収集した．ただし，1 つの記事に複数の事例が挙げられていたこともあったため，事例件数は 381 件となった．なお本研究での事故の定義は，システムが稼動後あるいは稼動前に品質，納期，コストのいずれかにおいて所定の要件を満たさないためにユーザクレームが発生し，システムの抜本的な見直しが必要になった事象とする．また，ユーザクレームが現に発生しなくても，明らかにユーザクレームの発生を予見できた場合も事故に含める．

次に収集した事故事例を整理してまとめ，そのうち本研究で使用できる事例と使用できない事例に分類した (3.1.3)．その結果本研究で利

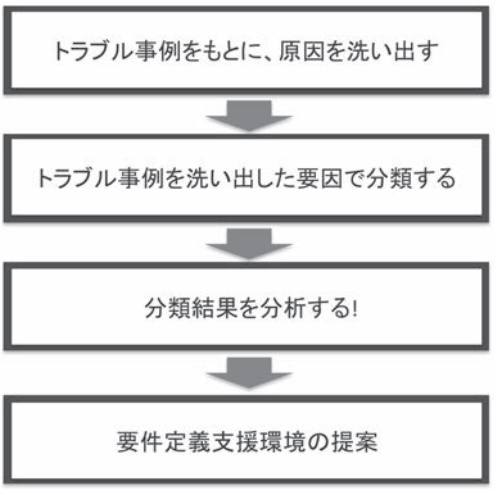


図 3_1. 事故事例分析から要件定義支援環境提案への手順

用できると判断した事故事例 270 件を，システム管理基準と情報セキュリティ管理基準を参照して要因ごとに分類した (3.1.4 と 3.1.5)．その後各要因に該当する事故事例の件数と復旧にかかった時間から要因の事故へのつながりやすさと重要性を分析する (3.2)．さらにそれらの要因と要件定義項目との関係を分析し (3.3)，1 そのうえで要件定義支援環境を提案する（4 節）．

3.1.3 事故事例の抽出

収集した事故事例に事例番号を付け，掲載されている雑誌の発行年月日，障害発生日，システム名もしくは関連する企業名，概要，回復までにかかった時間，影響規模，主な原因，その後の対応策についてまとめた（表 3_1）．

障害発生時間は，システムがすでに稼働している最中に事故が起こった場合は発生日時を，システムがまだ開発途中だった場合は開発を中断した日時，話し合いが拗れて裁判となった場合はどちらかが訴訟を起こした日時を記載している．回復時間はシステムの利用者が何らかの方法でシステムを利用できるようになるまでの時間であり，代替手段が用意されていた場合は代替手段が使用できるようになるまで，用意されていなかった場合はシステムが完全復旧するまでの時間となっている．影響規模はシステムの事故によって直接被害を受けた人数，損害金額，また何らかの被害規模が分かる数値を記載した．回復時間，影響規模ともに全ての事例で判明したわけではなく，それぞれ全体の 52%，47%の事例で判明した．事故事例の主な原因として企業が公表した情報，関係者・専門家による意見を収集し，雑誌編集者自身の推測に基づく記載は参照しないようにした．

381 件の事故事例のうち，情報システム開発に関わる事故事例として扱うことができる事例とできない事例に分別する．分類条件は 2 つあり，第 1 条件は事故の現象の概要や対策だけではなく，要因まで判明していることである．第 2 条件は要因が情報システム開発に関わっていることである．

① 第 1 条件を満たさない例

表 3_2 の事例は突如として Yahoo! のキーワード検索が止まってしまったという現象の概要のみ判明している事例である．この事例では対策，要因ともに判明していない．

表3_3 の事例は水道料金の督促を誤って送ってしまったという業務上現象や，プログラムにバグを作り込んでしまったという設計上の現象が判明しているが，プログラムにバグを作り込

表 3_1. 収集した事故事例のまとめ例

事例番号	発行年月日	障害発生時	システム/企業	概要	回復時間	影響規模	主な原因	その後の対策/その他メモ
64	2002/11/14	2002/9/3	トレンドマイクロ	契約更新者向けクレジット決済サイトで、アクセスが集中すると他の顧客の情報が誤って表示する不具合が発生した。	1ヶ月以上閉鎖	2万3000人	暗号化に使用していたツールに一定以上の負荷がかかると処理が遅延し、直前にログインした他の顧客の情報が誤って表示された。アクセス制限を行う設定になっていなかった。負荷テストが不十分だった。	第三者的な部署の監査を取り入れるなどしてセキュリティ対策を強化する

表 3_2. 第 1 条件を満たさない事例（事例番号 103）

事例番号	発行年月日	障害発生時	システム/企業	概要	回復時間	影響規模	主な原因	その後の対策/その他メモ
103	2004/1/26	2003/12/2	Yahoo!Japan Yahoo!キーワード検索	キーワード検索サービスが停止した。	3時間		原因不明	

表 3_3. 第 1 条件を満たさない事例（事例番号 49）

事例番号	発行年月日	障害発生時	システム/企業	概要	回復時間	影響規模	主な原因	その後の対策/その他メモ
49	2002/6/3	2002/4/1	愛知県豊田市	水道料金の督促をすでに振り込み終わっていた合計295の個人や企業に誤って送ってしまった。		295通	プログラムのバグ。	

表 3_4. 第 2 条件を満たさない事例（事例番号 179）

事例番号	発行年月日	障害発生時	システム/企業	概要	回復時間	影響規模	主な原因	その後の対策/その他メモ
179	2007/12/10	2006/6/20	構造計算プログラム	6月の建築基準法改正以降、中高層マンションなどの建築着工が大幅に落ち込んでいる。建築物の構造設計に不可欠な構造計算プログラムがいまだ改正法に対応できないでいる。			改正と同時に示すべきだった構造計算の具体的な手順や構造設計書の記載法の策定が遅れている。	

んでしまった要因までは判明していない事例である．

② 第 2 条件を満たさない例

表 3_4 の事例は中高層マンションなどの建築着工が大幅に遅れたために，建築物の構造設計に不可欠な構造計算プログラムがいまだに改正法に対応できないで いたというものである．改正と同時に示すべきだった構造計算の手順等の策定が遅れていたという要因が判明している．しかしこの要因は情報システム開発に直接関わる要因ではないため，本研究の対象事例としない．381 件の事故事例のうち，この 2 つの条件を揃えた事例 270 件を以降本研究の対象事故事例とする．

3.1.4 要因分類項目の設定

対象事故事例 270 件を事故の要因ごとに分類するために，要因分類項目を設定する．

要因分類項目の作成にあたっては，2.3 で述べたシステム管理基準並びに 2.4 で述べた情報セキュリティ管理基準を参照する．システム管理基準，情報セキュリティ管理基準では情報システムを企画から開発，運用，保守まで幅広く俯瞰しており，各フェーズで考慮すべきことが体系立てて整理されている．このシステム管理基準，情報セキュリティ管理基準を参照に分類項目を作成することで，各事故の要因の関連を整理することができ，ダブり漏れのない要件項目の作成ができると考えた．

本研究の要因分類では，システム管理基準の大項目である情報戦略，企画業務，開発業務，運用業務，保守業務，共通業務の 6 つを大項目に採用した．これに加えて，情報セキュリティ管理基準の全体に対応する大項目としてセキュリティという大項目を設け，合わせて 7 つの大項目に分けた．中項目には，システム管理基準の中項目および情報セキュリティ基準の大項目を採用した．そのうえで次項において述べる事故事例の要因分析を進め，事故の要因をグループ分けして小項目とし，その事故要因が所属すると思われる中項目の下位の層に配置した．この作業をすべての事故事例に対して実施し，グループ分けを見直しことで 76 の小項目を決定していった．なお，システム管理基準の中項目は 38 項目，情報セキュリティ基準の大項目は 11 項目であり，本研究の要因項目の中項目は 49 項目が存在することになるが，体系を単純化するため一つも事故要因が配置されなかった中項目は削除し，33 の中項目とした（表 3_5）．

3.1.5 事故要因の分類

例として，事例番号 348 と事例番号 6 の事故事例の分類について説明する．

事例番号 348 の事故事例の要因は，要件定義フェーズで性能要件を曖昧に決めてしまったことである (表 3_6). これは，要因番号 20「要求されるシステム性能を満たすために容量・能力に関する要求事項を特定し，また将来必要とされる容量・能力も予測する」に当てはまる．事例番号 348 の事故事例では，要求されるシステム性能を満たすために容量・能力に関する要求事項を明確に特定しなかったためである．

それに対して事例番号 6 の事故事例の要因は，事例番号 348 の事故事例と同じく性能に関することである．(表 3_7) しかしこちらは要件定義フェーズで性能要件が曖昧だったとの記述

表 3_5. 事故事例の要因分類項目

トラブル要因分類			要因番号
Ⅰ.情報戦略	1.全体最適化	経営環境の変化によってシステム化計画に影響を及ぼした	1
		システム化によって生じる現行業務の変更を明確にしなかった	2
	2.組織体制	組織体規模及び特性に応じて適切な職務の分離や権限及び責任の付与を行わなかった	3
	3.情報化投資	効果的に投資を行わなかった	4
	4.情報資産管理の方針	システム管理体制の不備	5
	5.コンプライアンス	遵守すべき法令及び規範の周知徹底を行わなかった	6
Ⅱ.企画業務	1.開発計画	開発計画は、目的、対象業務、費用、スケジュール、開発体制、投資効果などを明確にしなかった	7
		開発時の役割分担を明確にしなかった	8
		費用の算出基礎を明確にしなかった	9
		システムの特性及び開発の規模を考慮して形態及び開発方法を決定しなかった	10
	2.分析	ニーズ調査が不足していた	11
		現状分析が不足していた	12
		システムを導入するに伴って発生する可能性のあるリスク分析が不足していた	13
		システムの導入効果を定量的及び定性的に評価していなかった	14
		パッケージソフトウェアのユーザニーズとの適合性を十分に検討していなかった	15
	3.調達	開発を遂行するために必要な要員、予算、設備、期間などを確保できていなかった	16
Ⅲ.開発業務	1.システム設計	ユーザビリティを考慮していなかった	17
		DBをシステム特性に応じて設計していなかった	18
		データの整合性を確保できていなかった	19
		要求されるシステム性能を満たすために容量・能力に関する要求事項を特定し、また将来必要とされる容量・能力も予測する	20
		性能が要求定義を満たしていなかった	21
		運用性・保守性を考慮して設計していなかった	22
		他のシステムとの整合性を考慮していなかった	23
		障害対策を考慮していなかった	24
		誤謬防止、不正防止を考慮してシステムを設計していなかった	25
		ユーザ教育の方針とそのスケジュールを明確にしていなかった	26
	2.プログラミング	コーディング標準に適合していなかった	27
	3.システムテスト・ユーザ受入れテスト	テスト時に誰も誤りに気づかなかった	28
		テスト計画はユーザ及びテストの責任者が承認していなかった	29
		ユーザ受入れテストを行わなかった	30
		要求事項を網羅したテストケースを設定していなかった	31
		テストに開発当事者しか参画していなかった	32
		テスト手法が適切ではなかった	33
		本番とテスト時の環境が異なっていた	34
		本番運用を想定した負荷テストを行っていなかった	35
		ユーザ受入れテストにユーザ及び運用の担当者が参画していなかった	36
	4.移行	移行時にはリスクを分析し対策を検討すること	37
Ⅳ.運用業務	1.運用管理ルール	運用管理ルールを適切に定めていなかった	38
	2.運用管理	運用管理ルールを遵守できていなかった	39
		業務処理の優先度を考慮してジョブスケジュールを定めていなかった	40
		事故及び障害の報告体制及び対応手順を明確にしていなかった	41
		事故及び障害の内容を記録し、責任者に報告していなかった	42
		事故及び障害の原因を究明し、再発防止策を講じていなかった	43
		システムのユーザに対する支援体制を確立していなかった	44
	3.入力管理	入力の誤謬、不正を防ぐ対策が講じられていなかった	45
	4.データ管理	データ管理ルールを定め、遵守していなかった	46
	5.ソフトウェア管理	ソフトウェアの利用状況を記録し、定期的に分析していなかった	47
	6.ハードウェア管理	ハードウェア管理ルールを定め、遵守していなかった	48
		ハードウェアが想定されるリスクに対応できる環境に設置されていなかった	49
	7.ネットワーク管理	ネットワークの利用状況を記録し、定期的に分析していなかった	50
	8.建物・関連設備管理	設備設定を正確に行わなかった	51

Ⅴ.保守業務	1.保守手順	保守ルールを適切に定め、遵守しなかった	52
	2.保守計画	目的、範囲、方法、スケジュールなどを明確に定めて計画を立てなかった	53
	3.保守の実施	保守計画に基づいて保守を実施しなかった	54
	4.保守の確認	保守のテスト計画を適切に定め、テスト計画に基づいて実施しなかった	55
	5.移行	移行時にはリスクを分析し対策を検討すること	56
Ⅵ.共通業務	1.ドキュメント管理	ドキュメントの品質基準を適切に定めていなかった	57
	2.委託・受託	委託先の誤謬防止、不正防止対策の実施状況を把握し、必要な措置を講じていなかった	58
		委託先選定のプロセスに甘さがあった	59
		再委託防止のための対策を取っていなかった	60
		成果物の検収を適切に行っていなかった	61
	3.災害対策	災害時対応計画を適切に定めていなかった	62
		バックアップ方法及び手順を検証していなかった	63
		代替処理、復旧手続きを定め検証していなかった	64
Ⅶ.セキュリティ	1.物理的及び環境的セキュリティ	セキュリティを保つべき領域で、適切な入退管理をしていなかった	65
		セキュリティを保つべき領域で、許可されたもの以外の持ち込み、使用を禁止していなかった	66
	2.通信及び運用管理	ウイルス検知の仕組みを用意していなかった	67
		常に最新の攻撃に対応できるように定義ファイルなどの更新を実施していなかった	68
		ログの取得を行っていなかった	69
		ネットワークサービス合意書にセキュリティ要求事項を盛り込んでいなかった	70
		システムの実務管理者及び運用担当者の作業を記録していなかった	71
	3.アクセス制限	アクセス制御方針を確立していなかった	72
		パスワード選択時に正しいセキュリティ慣行に従うことを利用者に要求していなかった	73
	4.情報システムの取得、開発及び保守	情報漏洩の可能性を抑止していなかった	74
		システムに脆弱性を残していた	75
	5.情報セキュリティインシデントの管理	システムに関連する弱点がきちんと報告されなかった	76

はなく，出来上がったシステムの性能が性能要求を満たさなかったという事故事例である．そのため，この事故事例は要因番号 21「性能が要求定義を満たしていなかった」に分類される．このようにして対象事故事例 270 件を要因項目に分類した．なお，該当する要因項目が複数ある場合は，当てはまる要因項目全てに分類したため，要因項目の頻度合計は 382 となる．

3.2 要因分類に基づく事故の傾向分析

3.2.1 頻度の高い要因項目

76 の要因分類項目のうちの該当件数が 10 件以上の要因を図 3_2 に示す．最も該当件数が多かったのは要因番号 7「目的，対象業務，費用，スケジュール，開発体制，投資効果などを明確にしなかった」（大項目：企画業務，中項目：開発計画）の 32 件であった．これは全体 382 件のうちの 8.4% である．2 番目に多かったのは要因番号 31「要求事項を網羅したテストケースを設定していなかった」（大項目：開発業務，中項目：システムテスト・ユーザ受け入れテスト）の 22 件 (5.8%)，続いて 3 番目は要因番号

表 3_6. 分類例 [事例番号 348]

事例番号	発行年月日	システム名	概要	主な原因	その後の対策/その他メモ
348	2013/4/18	横浜市	横浜市が運営する18の図書館が利用する基幹システムでトラブルが発生。	性能要件が曖昧だった	

表 3_7. 分類例 [事例番号 6]

事例番号	発行年月日	システム名	概要	主な原因	その後の対策/その他メモ
6	2001/2/26	東京都交通局（東洋電機）	都営大江戸線全線開通から2週間、一部経路の定期券を発売できなかった。	当初開発したプログラムでは定期券を手早く発行できないことが判明、作り直したもののテストが間に合わず、直前になって発売を断念した。定期券発売機で新たなプログラムを動作させても十分な性能が得られると当初は考えていた。しかし処理の大きさが予想をはるかに超えていた。	

21「性能が要求定義を満たしていなかった」（大項目：開発業務，中項目：システム設計）ならびに要因番号 38「運用管理ルールを適切に定めていなかった」（大項目：運用業務，中項目：運用管理ルール）の 17 件 (4.5%) であった．特定の項目にあまり集中することはなく，幅広い分類の項目に要因が分析された．

3.2.2 公共システムの事故事例と民間システムの事故事例の対比

対象事例 270 件を省庁や自治体が調達した公共のシステムと民間が開発したシステムに分類し，７つの大項目で要因を分類すると図 3_3 の通りとなった．

公共のシステム開発の事故要因は，Ⅳ運用業務の割合が民間のシステム開発の事故要因よりも多かった．公共のシステムに分類された事故事例では，適切な運用管理ルールの不足，また運用管理ルールが遵守されていない事例が多かった．

民間のシステム開発の事故要因は，Ⅶセキュリティの割合が公共のシステム開発の事故要因よりもかなり多かった．特にウイルス検知の仕組みを用意しておらず感染してしまった事例や，システム内の脆弱性を放置したまま対処していなかった事例が目立っていた．

3.2.3 復旧時間による分析

対象事例 270 件の復旧時間を，6 時間以内，12 時間以内，24 時間以内，1 週間以内，1 ヶ月以内，1 ヶ月以上の 6 段階に分けて分類する．6 時間以内の事例には 1，12 時間以内の事例には 2，24 時間以内の事例には 3，1 週間以内の事例には 4，1 ヶ月以内の事例には 5，1 ヶ月以上の事例には 6 の点数をつける．この値を復旧時間指標と呼ぶことにする．復旧時間指標を

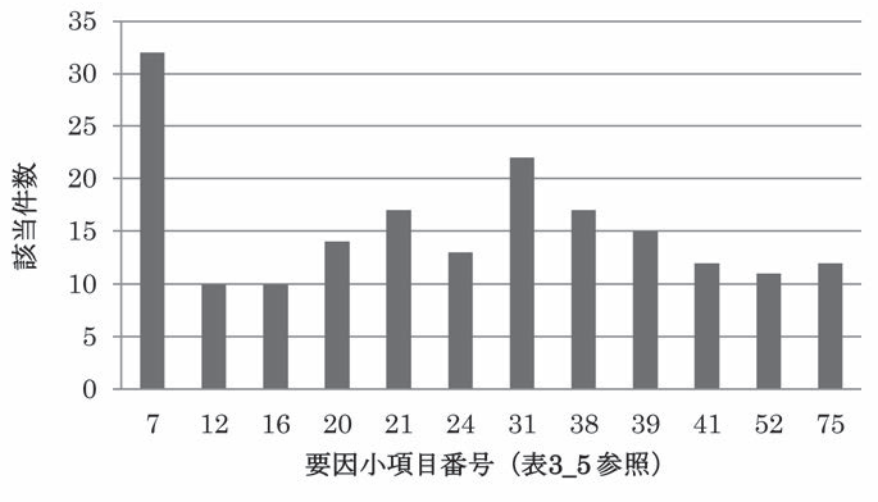


図 3_2. 頻度の高い要因項目（該当件数が 10 以上の要因）

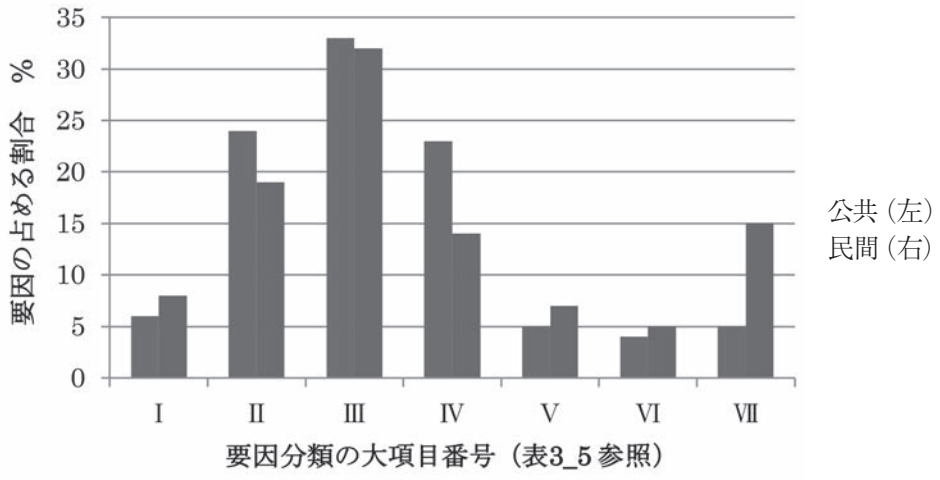


図 3_3. 要因の占める割合 [公共民間別]

要因ごとに平均を算出し、要因ごとに 1 から 6 までの値を出す．6 に近いほど復旧に時間がかかった要因である．76 の要因のうち事例の件数が 3 件未満の要因を除き，復旧時間指標の平均値が 4 以上の要因は図 3_4 の通りである．

復旧時間指標の平均値が特に高かったのは要因番号 75(5.45 点) システムに脆弱性を残していた，と要因番号 45(5.33 点) 入力の誤謬，不正を防ぐ対策が講じられていなかった，でありどちらも 5 点を超えていた．

要因番号 75 に該当する事例では，システムの脆弱性を突かれて外部から不正に侵入され，web サイトを改ざんまたは会員情報が漏洩する事例が多かった．そのため，システムの全面改修やセキュリティ体制を万全にするためにすぐに復旧させることができず，時間がかかっている．

要因番号 45 に該当する事例では，膨大な量のデータを扱うシステムで誤入力のチェックを行う機能が欠けていた事例や，新旧漢字が入り混じってしまいデータの整合性が保てず，システムが動かなくなる事例があった．膨大な量のデータの整合性を確保し，システムを適切に運用できるようになるまでに時間がかかってい

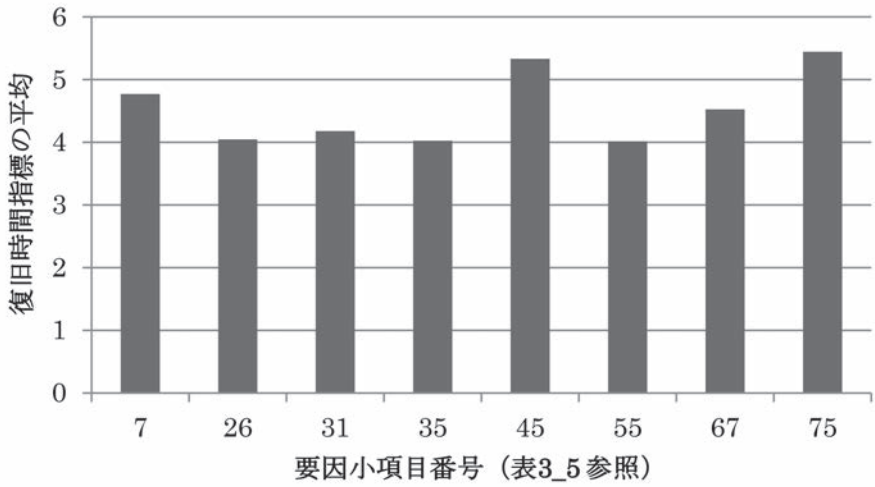


図 3_4. 復旧時間指標の大きい要因（4 以上の要因）

る.

3.3 事故の要因項目と関連するシステム要件定義項目

要因分類項目に，要件定義書において関連する要件定義項目と，要件定義項目を記述する際に参考となる資料を紐付け，「要因項目と要件定義項目の対応表」を作成した (表 3_8). 要件定義項目は 2.2 で述べた要件定義項目を用いた．参考となる資料は 2.5 で述べた TRM 物品調達編および TRM 役務調達編の項目，2.6 で述べた非機能要求グレードの項目を用いた.

3.3.1 対応する要件定義項目がない事故の要因項目

要因項目と要件定義項目の対応表では，対応する要件定義項目がない要因が 9 つ存在する．要因番号 1，6，21，28，31，39，51，54，55 の 9 つである．これらの要因は人為的なミスや規則違反による要因であり，要件定義フェーズで防ぐことは難しい.

3.3.2「要因項目と要件定義項目の対応表」例

参考資料との対応付けの例として，要因番号 20，38，69 の３つを説明する.

●事故の要因項目に関連する非機能要求グレードの例

表 3_8. 要因項目、要件定義項目および参考資料の対応（抜粋）

要因番号	要件定義該当箇所	参考資料		
		非機能要求グレード	TRM 役務調達編	TRM 物品調達編
1	該当項目なし			
2	業務要件定義		2.3 システム構築（設計・開発）	
3				
4				
5	運用要件定義		2.4 運用	
6	該当項目なし			
7	機能要件 スケジュール定義		2.3 システム構築（設計・開発）	
8	設計・開発要件定義		2.3 システム構築（設計・開発）	
9	契約事項			
10	設計・開発要件定義		2.3 システム構築（設計・開発）	
11	業務要件定義		2.3 システム構築（設計・開発）	
12				
13				
14				
15				
16	設計・開発要件定義		2.3 システム構築（設計・開発）	
17	機能要件定義 （情報・データ）			
18				
19	非機能要件定義 （信頼性・性能）	運用保守性 インシデント管理		
20		性能・拡張性 業務処理量、リソース拡張性		
21	該当項目なし			
22	非機能要件定義（信頼性）	運用・保守性　運用負荷軽減		
23	機能要件定義			
24	非機能要件定義（信頼性）			
25	機能要件定義			
26	移行要件定義	移行性	2.3. システム構築(設計・開発) 2.7 機器調達付帯作業　9.利用者への情報提供・教育	

最初に，要因番号 20「要求されるシステム性能を満たすために容量・能力に関する要求事項を特定し，また将来必要とされる容量・能力も予測する」という要因である場合について解説する．この要因が関連する要件項目は，非機能要件の性能要件である．性能要件に関わる参考資料としては，非機能要求グレードの性能・拡張性の業務処理量であるユーザ数，同時アクセス数，データ量，オンラインリクエスト件数, バッチ処理件数を用いることができる．（表 3_9）

ここで，ユーザ数に関して，もし部門内利用等でユーザが特定できる場合は 1 番左のレベル 0「特定ユーザのみ」を選択し，あらかじめ一定の上限値を設定することが可能である場合は 2 番目のレベル 1「上限が決まっている」を選択する．国民全体がアクセスする可能性があるような場合は 3 番目のレベル 2「不特定多数のユーザが利用」を選択して，それぞれ要件定義書に記述することになる．

●事故の要因項目に関連する TRM 役務調達編の例

次に，要因番号 38「運用管理ルール，運用管理ルールを適切に定めていなかった」という要因の場合について解説する．この要因が関連する要件定義項目は，非機能要件の運用要件である．運用要件に関わる資料としては，TRM 役務調達編の「2.4 運用 1. 運用計画の策定」が該当する．(表 3_10)

「2.4 運用 1. 運用計画の策定」では主として運用計画書と運用手順書，体制表作成について述べている．発注者側でスケジュール, 運用要領, 役割分担，サービスレベル項目などを定め，受注者側ではそれを元に運用計画書，運用手順書などを作成することや，その他にも仕様書に記載するべきポイント, 仕様書記載上の例と説明, 案件・情報システムの特性などによる留意点, セキュリティに関する留意点などが記載されている．

●事故の要因項目に関連する TRM 物品調達編の例

最後に，要因番号 69「通信および運用の管理，ログの取得を行っていなかった」という要因の場合について解説する．この要因が関連する要件項目は，非機能要件の情報セキュリティ要件である．情報セキュリティ要件に関わる資料としては，TRM 物品調達編の「2.17. セキュリティ」が該当する．「2.17. セキュリティ」にはセキュリティに関連する様々な機能・サービスの要件定義に関する記述が含まれており，要

表 3_9. 非機能要求グレード「性能・拡張性」[3]（抜粋）

大項目	中項目	小項目	メトリクス（指標）	レベル			
				0	1	2	3
性能・拡張性	業務処理量	通常時の業務量	ユーザ数	特定ユーザのみ	上限が決まっている	不特定多数のユーザが利用	
			同時アクセス数	特定利用者の限られたアクセス	同時アクセスの上限が決まっている	不特定多数のアクセス有り	
			データ量	すべてのデータ量が明確である	主なデータ量のみが明確である		
			オンラインリクエスト数	処理毎にリクエスト数が明確である	主な処理のリクエスト件数のみが明確である		
			バッチ処理件数	処理単位ごとに処理数が決まっている	主な処理の処理件数が決まっている		

表 3_10 TRM 役務調達編「2.4 運用，1. 運用計画の策定」[3]（抜粋）

項目	内容
役務内容の概要	運用の実施計画を策定し、運用計画書を作成した上で、府省担当課の承認を得る。
想定されるインプット （発注者側で用意）	全体スケジュール 運用要領 運用設計書 体制図（当該システムの関連事業者、発注者） 役割分担（当該システムの関連事業者、発注者） 運用対象システムの概要 運用対象システムの構成情報 担当運用業務の内容・業務量等の要件 サービスレベル項目 等
成果物 （受注者側で用意）	運用計画書 運用手順書 体制表 等 サービスレベル項目／定義書案 （府省によっては導入計画書、体制表等ドキュメントを分けて提出を求める場合も存在する。こうした点に関しては各府省で定められている調達方針・ガイドラインに沿う事が望ましい。）
仕様書に記載すべきポイント	設計・開発事業者、現状の運用事業者と調整の上、以下の内容を含む運用作業の実施計画を策定する 【1.基本的に記載すべき要求要件】 ・実施すべき作業内容 ・実施体制における役割分担、指示・命令系統 ・作業時間帯、作業場所等に関する指定及び制約条件 ・プロジェクトマネジャ、リーダ、担当者に求められる要件（スキル・経験・資格） ・担当者の届出、変更の場合のルールの遵守 等 ・サービスレベル 【2.案件の種類・特性によって追記すべき要求要件】 ・運用環境構築等、付帯業務が発生する場合当該業務に関する計画
仕様書記載上の例/説明	仕様書に記載する場合の例 ○実施体制等 ① 受託者は落札決定後7 日以内に運用計画書(スケジュール､実施体制 等を含む)を作成し､主管課に納入の上､承認を得ること。 ② 受注者は、本業務の実施に当たって、本業務に従事する運用支援要員２名以上、運用支援要員をサポートする補助要員２名以上の実施体制を整備し、その体制表に運用支援要員及び補助要員の所属・役職・氏名・連絡先を添えて担当職員に提出すること。 ③ 運用支援要員及び補助要員は、○○課に常駐し、本業務を実施すること。 ④ 受注者は、受注者側の事情により、運用支援要員及び補助要員を変更する場合は、変更する日の2 週間以上前までに担当職員と協議すること。 ⑤ 運用支援要員及び補助要員の変更を行う場合、受注者は引継書を作成し、十分な引継ぎ、トレーニングを行い、業務に支障を来さないようにすること。
案件・情報システムの特性等による留意点	① 設計・開発事業者において運用計画を策定しているケースも存在する。その場合、設計開発事業者と調整の上計画を確定させる必要あり。 ② 継続や追加調達等、既存の運用事業者との調整や既存の運用計画との連携・調整が必要な場合はその旨を記載する必要あり。 ③ 作業場所が複数にわたる場合や再委託が必要な場合などにはその旨を記載し、役割分担や責任範囲を明確にする。
セキュリティに関する留意点	体制図等に個人情報の記載がある場合、当該文書は規程に定める重要度に応じた取り扱いとする。

因番号 69 に対応して，「2.17.5.3. セキュリティログ管理機能」が設けられている．(表 3_11)

「2.17.5.3. セキュリティログ管理機能」はファイアウォールや不正侵入検知機能などのログを収集，分析し，セキュリティを管理する機能である．機能要件として 4 つの基本要件，非機能要件として 2 つの基本要件が述べられており，セキュリティログ管理機能を情報システムに搭載する際には，これらの要件を満たすことが必要であると述べている．

4 要件定義支援環境の提案

4.1 システムの構成

本研究で作成する要件定義支援環境の利用対象者は，要件定義書を記述しようとしている人と要件定義について学ぼうとする人である．要件定義書を記述しようとしている人が PC 上で他のアプリケーションの画面を開きながら参照することを想定し，PC 上で閲覧する Web システムとして構築する．(図 4_1)

要件定義を実施するためには情報システム構築に関する幅広い知識が必要であるが，要求定義の学習者はもとより，要件定義業務の担当者においても必ずしも十分な知識や経験を有している場合ばかりではない．そこで，要件定義に必要な知識を簡便且つ網羅的に取得し，要件定義の大きな漏れを防止することが重要となる．本研究提案の支援環境においては，要件定義のひな形や TRM などの参考資料とともに事故要因別に整理された事故事例情報を提供し，システム開発のリスクを低減することを狙いとする．

ユーザは PC から要件定義支援環境にアクセスし，メインメニューから要件定義書のひな型をダウンロードすることができる．要件定義に関する情報を閲覧したい要件定義項目（以下，要件項目と略す）を選択し各要件項目のページを開くと，各要件項目に該当する要因，その要件項目を記述する際に参考となる資料へのリンク，実際に調達が行われた政府の調達仕様書の該当箇所へのリンク，その要件項目への取り組みが不十分であったために発生した事故事例の一覧をみることができる．

参考資料としては，各要件項目に該当する TRM と非機能要求グレードのページが表示される．記述参考例としては，インターネット上で公開されている実際に調達が行われた政府の調達仕様書のうち，総務省から提供されている情報システムに係る政府調達指針に沿って調達が行われたものだと思われる調達仕様書を選んで，その該当箇所を表示している．事故事例としては，日経コンピュータで掲載されている「動かないコンピュータ」で取り扱っている事故事例の記事について概要をまとめたものを掲載している．

本研究では，このような要件定義支援環境の利用モデルと機能詳細を設計した．さらに画面機能や参考資料等のコンテンツを一部実装

表 3_11.TRM 物品調達編「2.17.5.3 セキュリティログ管理機能」[2]

要件種別	要件項目	基本／加点	内容
機能要件	1	基本	ファイアウォールや不正侵入検知機能等のログを収集できること。
	2	基本	Webサーバ等のイベントログ等の情報を収集できること。
	3	基本	収集したログを一元的に管理できること。
	4	基本	権限を有する管理者は、収集したログの検索、分析が行えること。
非機能要件	可用性	基本	冗長構成が可能であり、故障時の自動切替が可能であること。
	セキュリティ	基本	収集後のログが改ざんされないこと。

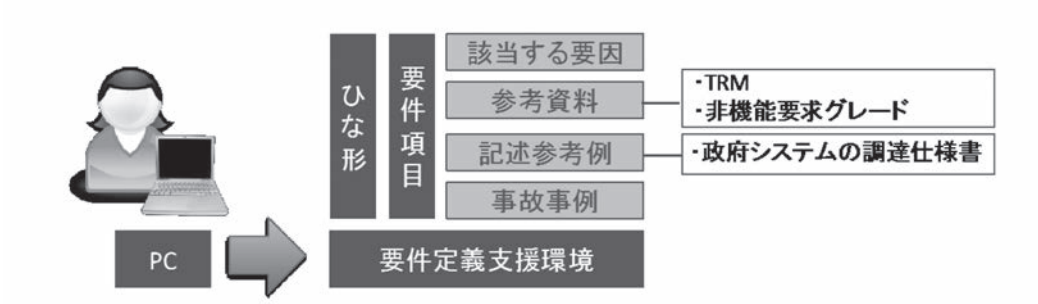


図 4_1. システム構成図

し，専門家等へのレビューを行った (第 5 節).

4.2 要件定義支援環境の利用モデル

対象利用者のうち，要件定義書を記述しようとしている利用者の利用モデルの一例を示す．(図 4_2)

利用者はまず要件定義支援環境で要件定義を記述するために，要件定義支援環境から要件定義書のひな形をダウンロードする．①ひな形に含まれる要件項目を記述するために参照したい要件項目を選択し，②事故要因一覧，参考資料，参考記述，事故事例一覧の中から閲覧したいものを選ぶ．③事故要因の一覧からは，その要件項目に関連が深い事故要因を知ることができる．参考資料からはその要件項目に何を書くべきかを知ることができ，参考記述では書くべきことの書き方を学ぶことができる．事故事例の一覧からは過去の失敗例を学び，④自分の要件定義書における要件項目の記述に生かすことができる．②〜④を要件項目ごとに繰り返すことによって，要件定義書の記述を完成させる．

4.3 要件定義支援環境の機能詳細

要件定義支援環境の画面構成は左右に分かれており，左側には常にメニューリストを，右側には本文が表示される構成となっている．

4.3.1 メニューリスト

メニューリストは項目数が多いため，親子関係を持つツリー構造となっている．親メニューはテンプレート（ひな形), 業務要件, 機能要件, 非機能要件の 4 つから構成されている．4 つのメニューにはそれぞれ 2 〜 9 の子メニューがあり，親メニューがクリックされた場合に表示非表示が入れ替わるようになっている (図 4_3).

子メニューには事故要因となりやすい項目に赤色，黄色，青色の星印が付いている．星印の数は事故要因へのつながりやすさ，事故事例

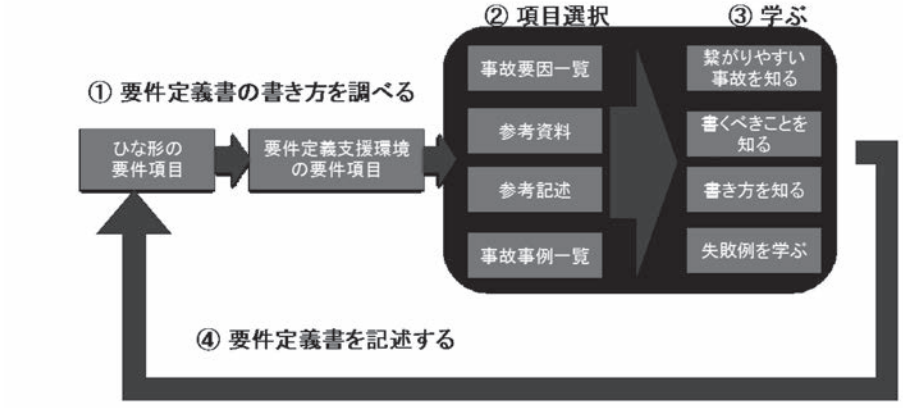


図 4_2. 要件定義支援環境の利用モデル

の多さを表している．星印の色は，事故が発生した場合，復旧するまでにどれくらいの時間がかかったかという影響度を表している．事故事例の多さは 3.2.1 で述べた頻度を参考にしている．3.2.1 で述べた頻度は要因項目ごとの頻度であるため，3.3 で述べた要因項目と関連する要件項目を参考に要件項目ごとの頻度に変換した．要件項目に該当する事故事例を１の位で四捨五入し，１０件ごとに星印を１つを付けている．復旧にかかった時間については 3.2.3 で述べた復旧時間を参考にしている．こちらも要因項目ごとの復旧時間であるため，3.3 で述べた要因項目と関連する要件項目を参考に要件項目ごとの復旧時間に変換した．1 から 6 の点数が付いている要件項目のうち，4 点以上の項目で星印が付いている項目は星印を黄色のに，5 点以上の項目で星印が付いている項目は星印を赤色に変更する．4 点以下の項目で星印が付いている項目は星印を青色とし，重要度が高い順に赤色，黄色，青色となるようにした．

親メニューの１つであるテンプレートでは，要件定義書を作成するためのひな形をダウンロードすることができる．TRM の関連資料としては，３つの調達対象のタイプに合わせた要件定義書のひな形（システム開発調達仕様書のひな形 [26]，運用管理支援調達仕様書のひな形

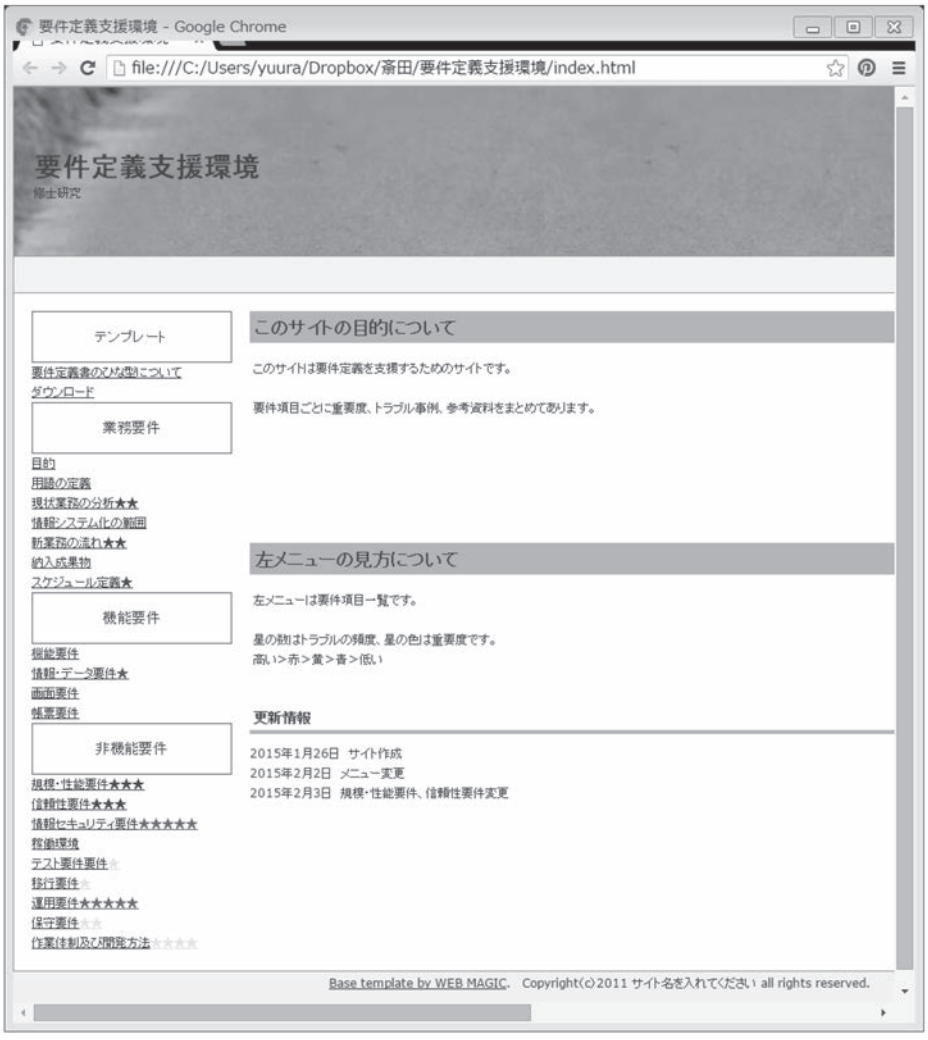


図 4_3. 要求定義支援環境のトップ画面

信頼性要件

信頼性要件とは...

システムの可用性、保守性、完全性などに関する要件のことである。例えば、業務が停止するほどの障害が発生した際に、何をどこまで、どれ位回復させるかを定める目標回復水準が当てはまる。

トラブル要因の一覧

•データの整合性を確保できていなかった→事例

・システムの統合、設定変更、旧システムから新システムへの移行時に起こりやすいトラブル。

・テスト不足、開発・移行スケジュールが短すぎるなどの要因とつながりやすい。

・稼動前に発生した場合、稼動予定が大きくずれることとなる。また、システムがエラーを検知しない場合、長期間にわたって利用しない場合もある。

•運用性・保守性を考慮して設計していなかった→事例

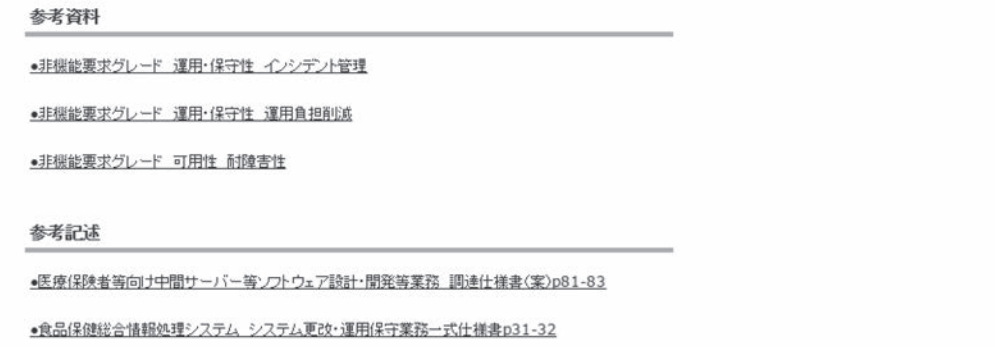
・設計時に、実際にシステムを利用するユーザ側の視点が欠けている。

•障害対策を考慮していなかった→事例

・冗長化不足によってシステムトラブルへと繋がった事例が多い。冗長化していなかった理由としては、故障する可能性を考えていなかったという事例と、コストを下げるためという事例の2つが挙げられる。

・通常時と障害時のデータの処理方法が異なっており、障害時に待機系への切り替えに成功したにも関わらず通常時よりも複雑な障害時の処理手順によってダウンした事例もある。

(a)事故要因の一覧



参考資料

•非機能要求グレード　運用・保守性　インシデント管理

•非機能要求グレード　運用・保守性　運用負担削減

•非機能要求グレード　可用性　耐障害性

参考記述

•医療保険者等向け中間サーバー等ソフトウェア設計・開発等業務　調達仕様書(案)p81-83

•食品保健総合情報処理システム　システム更改・運用保守業務一式仕様書p31-32

(b)参考資料の一覧および参考記述の一覧

トラブル事例一覧

•データの整合性を確保できていなかった

事例番号	発行年月日	システム名(関連企業)	概要	主な原因
119	2005/12/26	ルネサステクノロジ（日立情報システムズ、三菱電機情報ネットワーク、アクセンチュア）	基幹システム統合が難航。当面延期する。	データベースの統合に手間取っている。
214	2007/8/6	日本社宅サービス 社宅管理システム（日本システムウエア）	再構築が難航、稼働が2年以上遅れた。開発費の負担を巡って訴訟にまで至ったが、最終的には和解した。	機能要件がかたまらなかった、メンバーの引き継ぎが不十分、データの整備付属、データの整備に関して関者の意見が一致しない。
272	2009/12/9	日本赤十字社 個人情報管理システム（クレオ）	骨髄バンクに登録しているドナーの一部を4年間にわたり正常に登録できていなかったことを公表した。	データベース間のデータ受け渡しにおけるプログラムのバグ。メインのデータベースの周辺にサブのデータベースが多すぎる。すべてその連結部分で不具合が生じている。全体を通したテスト不足
353	2013/5/16	住民基本台帳ネットワークシステム	39都道府県1500市町村で障害が発生。231市町村でデータ更新に文字化けが発生。1500市町村で利用できなくなった。	データベース設定変更時のミス
358	2013/5/30	仙台市 市民利用施設予約システム（富士通とそのグループ会社）	2013年1月に稼動を予定していたシステムが6月中旬でも稼動していない。	前システムからのデータ移行に不備が発生。仙台市の特殊なデータ構造をベンダーが把握しきれていなかった。
371	2014/5/1	ひめ	約3億円分のクレジットカード決済の代金を二重請求する障害が発生。	データベースの構成変更が原因。DBを刷新して負荷分散を図った結果、処理のタイミングによってデータに不整合が発生した。

(c) トラブル事例の一覧（抜粋）

図 4_4. 各要件項目画面（信頼性要件項目）

[27]，機器賃貸借及び保守調達仕様書のひな形[28]）が公開されているので，これらをダウンロードすることができるようにした．

同じく親メニューの 1 つである業務要件には，システム開発の目的，ユーザとベンダーの間で解釈が異なりやすい用語の定義，現行または新業務の分析，システム化の範囲，納入成果物，システム開発全体のスケジュールに関わる子メニューが含まれている．

非機能要件には，システムの品質に関わる規模･性能要件，信頼性要件，情報セキュリティ要件，稼働環境に加えて，情報システムの開発･運用・保守に関わる作業体制及び開発方法，テスト要件，移行要件，運用要件，保守要件が子メニューとして含まれている．

4.3.2 各要件項目画面

業務要件，機能要件，非機能要件に含まれている子メニューを選択すると，各要件項目のページを閲覧することができる．この各要件項目のページは，①事故要因の一覧，②参考資料，③参考記述，④事故事例一覧の 4 つのコンテンツで構成されている (図 4_4).

① 事故要因の一覧

事故要因の一覧では，3.3 で述べた要因項目と関連する要件項目を参考に，各要件項目に関連する事故要因の一覧が記載されている．例として非機能要件の信頼性要件では，要因番号 19「データの整合性を確保できていなかった」，要因番号 22「運用性・保守性を考慮して設計されていなかった」，要因番号 24「障害対策を考慮していなかった」の 3 つの要因が該当する．さらに各要因の事故事例の特徴をまとめて記載している．

② 参考資料

参考資料には，各要件項目を記述する際に参考となる TRM と非機能要求グレードの該当箇所へのリンクを記載している．例として，非機能要求の信頼性要件では非機能要求グレードの運用・保守性に含まれるインシデント管理と運用負担削減，同じく非機能要求グレードの可用性に含まれる耐障害性が参考資料として挙げら

システム基盤の非機能要求に関する項目一覧

項目一覧

項番	大項目	中項目	小項目	小項目説明	定性/定量項目	選択/必須項目	メトリクス(指標)	レベル 0	レベル 1	レベル 2	レベル 3	レベル 4	レベル 5	既存システムからの移行	備考
C.5.1.1			サポート要員	サポート体制に組み入れた要員の人数や対応時間、スキルレベルに関する項目。			ベンダ常年運転要員人数	常駐しない	1人	複数人					
C.5.2.1							ベンダ常対応時間帯	対応無し	ベンダの定時時間内(9～17時)	夜間のみ非対応(9～21時)	形態(時間)に時間帯を非対応有り(9～翌9時)	24時間対応			
C.5.3.1							ベンダ常対応者の要求スキルレベル	指定無し	有識者の指導を受けて機器の操作を実施できる	システムの構成を把握し、ログの収集・確認が実施できる	システムの運用や保守業務に習熟し、ハードウェアやソフトウェアのインナンス作業を実施できる	システムの開発や構築業務に携われ、業務者や ユーザの意図にも通じている			
C.5.4.1							エスカレーション対応	指定無し	オンコール待機	第2待機	現地待機				[メトリクス] 障害発生時にエスカレーション対応が必要となるSIパートや製品に関して、エスカレーション先の有識者の待機方法について確認する。
C.5.7.1			導入サポート	システム導入時の特別対応期間の有無および期間。			システムテスト段階時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上			
C.5.7.2							システム移行後時の導入サポート期間	無し	当日のみ	1週間以内	1ヶ月以内	1ヶ月以上			
C.5.8.1			オペレーション訓練	オペレーション訓練実施に関する項目。			オペレーション訓練実施の任意/計画	実施しない	全てユーザが実施	一部ユーザが実施	全てベンダが実施				
C.5.8.2							オペレーション訓練範囲	実施しない	通常運用の訓練を実施	通常運用に加えて保守運用の訓練を実施	通常運用、保守運用に加えて、障害発生時の復旧作業に関する訓練を実施				[レベル] 通常運用とは、システム基盤における通常時の運用(起動・停止等)にかかわる操作を指す。保守運用とは、システム基盤における保守作業(製品交換やデータ復旧手順等)にかかわる操作を指す。
C.5.8.3							オペレーション訓練実施頻度	実施しない	システム立ち上げ時のみ	定期開催					
C.5.9.1			定期報告会	保守に関する定期報告会の開催の要否。			定期報告会実施頻度	無し	年1回	半年に1回	四半期に1回	月1回	週1回以上		[メトリクス] 障害発生時に実施される不定期の報告会はネットリクスには含まない。
C.5.9.2							報告内容のレベル	無し	障害報告のみ	障害報告に加えて運用状況報告を行う	障害および運用状況報告に加えて、改善提案を行う				
C.6.1.1		その他の運用管理方針	内部統制対応	IT運用プロセスの内部統制対応を行うかどうかに関する項目。		○	内部統制対応の実施有無	内部統制対応について確定しない	既存の社内規定等に従って、内部統制対応を実施する	新規に規定や体制、プロセスを策定し、内部統制対応を実施する					[メトリクス] ここでは、内部統制対応の実施有無について確認する。内部統制対応の具体的な対応方法(オペレーションで実施するか、システムへの機能実装で実現するか等)については、有無の確認後に具体化して確認する。
C.6.2.1			サービスデスク	ユーザの問合せに対して単一の窓口機能を提供するかどうかに関する項目。		○	サービスデスクの設置有無	サービスデスクの設置について確定しない	既存のサービスデスクを利用する	新規にサービスデスクを設置する					[メトリクス] ここでは、ユーザとベンダ間におけるサービスデスクの設置の有無について確認する。サービスデスク機能の具体的な実現方法については、有無の確認後に具体化して確認する。
C.6.3.1			インシデント管理	重要な停止させるインシデントを迅速に回復させるプロセスを実施するかどうかに関する項目。			インシデント管理の実施有無	インシデント管理について確定しない	既存のインシデント管理のプロセスに従う	新規にインシデント管理のプロセスを構築する					[メトリクス] ここでは、組織システムで発生するインシデントの管理を実施するかどうかを確認する。インシデント管理の実現方法については、有無の確認後に具体化して確認する。
C.6.4.1			問題管理	インシデントの根本原因を追究し、可能であれば恒久策とための効果を図るプロセスを実施するかどうかに関する項目。			問題管理の実施有無	問題管理について確定しない	既存の問題管理のプロセスに従う	新規に問題管理のプロセスを設定する					[メトリクス] ここでは、インシデントの根本原因を追究するための問題管理を実施するかどうかを確認する。問題管理の実現方法については、有無の確認後に具体化して確認する。
C.6.5.1			構成管理	ハードウェアやソフトウェアなどの構成情報を適切に管理するためのプロセスを実施するかどうかに関する項目。			構成管理の実施有無	構成管理について確定しない	既存の構成管理のプロセスに従う	新規に構成管理のプロセスを設定する					[メトリクス] ここでは、リリースされたハードウェアやソフトウェアが適切にユーザ環境に構成されているかを管理するための構成管理を実施するかどうかを確認する。構成管理の実現方法については、有無の確認後に具体化して確認する。

図 4_5. 参考資料の表示 (非機能要求グレード [4] の信頼性要件関連部分)

れる．そのうちの１つである非機能要求グレードの運用・保守性 インシデント管理を選択すると，非機能要求グレードの関連するページがpdf で表示され，該当箇所には利用者がわかりやすいように赤で印が付けられる (図 4_5).

③ 参考記述

参考記述として，実際に公官庁や自治体が作成した情報システムの調達仕様書の該当箇所へのリンクを記載している．例として，非機能要求の信頼性要件では厚生労働省が作成した医療保険者向け中間サーバー等ソフトウェア設計・開発等業務調達仕様書（案）[29] の p81 から p83 までと，同じく厚生労働省が作成した食品保健総合情報処理システム システム更改・運用保守業務一式仕様書 [30] の p31 から p32 までへのリンクを記載している．

④ 事故事例一覧

事故事例一覧では，要件項目に関連する各要因に該当する事故事例の一覧を掲載している．この事故事例は本研究で対象事例として取り上げている日経コンピュータの動かないコンピュータを著者の一人が読み，概要をまとめたものである．具体的には事故事例が発生した年度順に事例番号を付け，事故事例の記事が記載されている雑誌の発行年月日，システム名，概要，主な原因の要点を短く整理して記載している．

5 事故要因の特徴と支援環境の評価

5.1 要件定義フェーズにおける事故要因の特徴

3.2.1 で述べた事故事例の要因ごとの頻度より，事故につながりやすい要因の特徴を考察する．ただし，要件定義フェーズに関連しない要因はこの考察の対象外として除いている．3.2.1 で述べた該当事例件数が 10 件を越す 12 の要因のうちでは，3 つの要因 (要因番号 21,31, 39) が要件定義フェーズ外であるので，そのほかの 9 つの要因（要因番号 7, 12, 16, 20,24, 38, 41, 52, 75）を該当事例件数と復旧にかかった時間で 4 つのグループに分類する (図 5_1).

図 5_1 の縦軸は該当した事例件数であり，縦軸の 15 件の位置に引かれた太線は、この 9 つの要因における平均事例件数を示す線である．横軸は復旧時間指標である．横軸の 3.5 の位置に引かれた太線は，3 件以上の要因全体の復旧時間指標の平均値を示す線である．グループ①は復旧に時間がかかる事故が起こりやすい要因である．グループ②は復旧にはさほど時間

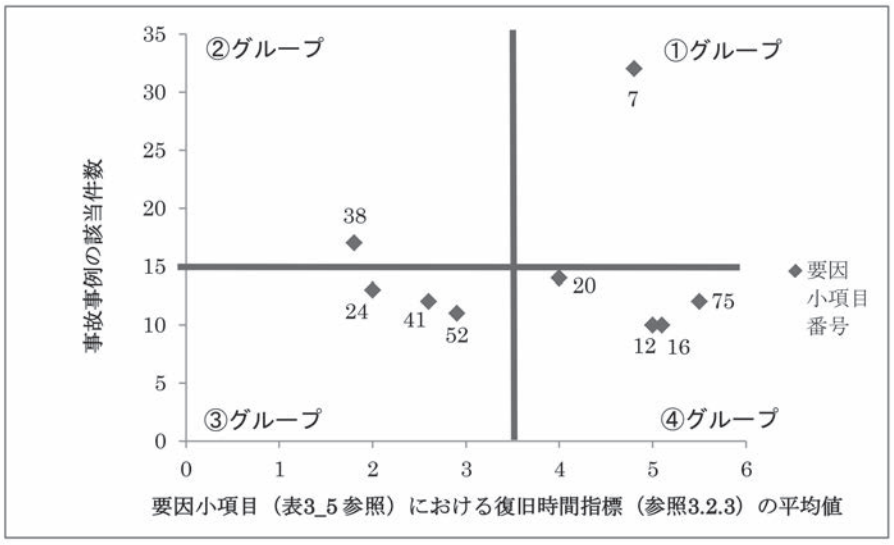


図 5_1. 事故要因の頻度と復旧時間による分布

がかかっていないが，よく事故につながりやすい要因である．グループ③は 4 つのグループの中では最も重要度が低く，復旧にかかった時間も頻度もこの 4 つのグループ内で 1 番低い．グループ④は事故の起こりやすさはこの 4 つのグループの中では高くはないが，復旧に 1 番時間がかかった要因が含まれている．

5.1.1 ①復旧に時間がかかる事故が起こりやすい要因グループ

グループ①に含まれている要因は 1 つだけであり，要因番号 7「開発計画は，目的，対象業務，費用，スケジュール，開発体制，投資効果などを明確にしなかった」である．期日までに要求仕様が固まらない，総合テストの段階になってから仕様の変更が出たという事例が当てはまった．

事例の多くが稼動予定日を半年から 3 年半ほど過ぎた後にプロジェクトを中断，もしくは稼動予定日が決まらないまま開発を続けており，その後システムが稼動したという事例は約 1 割しかない．またその 1 割の事例も，稼動こそしたものの 1 年以上バグを抱えたまま業務に深刻な影響が生じていた事例や，予定していたシステムの一部しか稼動していないという事例がほとんどを占めている．

突然大きなトラブルに見舞われるわけではなく少しずつ費用と納期が計画から外れるため，システム開発を中止するという大きな決断が困難である．従って，トラブルが長期化しやすく，また大きな事故事例にかなりつながりやすい要因であると考えられる．

5.1.2 ②復旧にさほど時間がかからない事故が起こりやすい要因グループ

グループ②に含まれている要因も 1 つだけであり，要因番号 38「運用管理ルールを適切に定めていなかった」である．利用頻度の低いシステムのマニュアルに不備があり，担当者が操作ミスを起こしトラブルへとつながる事例があてはまった．

この事例には官公庁や地方自治体が市民に提供する公共的なシステムが多くあてはまった．通常運用時の使いなれた操作は多少マニュアルに不備があっても問題はあまり発生しないが，年に数度の訓練時や新業務などで使いなれないシステムを職員が利用する場合には手順書のわずかな記載漏れがトラブルにつながるのだと考えられる．滅多に使用しないシステムや機能ほど，丁寧なマニュアルが必要である．

5.1.3 ③復旧にかかる時間も事故の頻度もさほど多くはない要因グループ

グループ③に含まれている要因は 3 つあり，要因番号 24「障害対策を考慮していなかった」，41「事故及び障害の報告体制及び対応手順を明確にしていなかった」，52「保守ルールを適切に定め，遵守しなかった」である．

この 3 つに共通することは，予測不足である．故障するとは思われていなかった装置が故障をした，想定していない事故が発生したために対応マニュアルが用意されていなかった，保守ルールがないため現場で十分な確認を行わずに作業を行い想定外のトラブルを引き起こしてしまった，という事例が当てはまった．また，わずかな例ではあるが，事故を想定して復旧手順や対応手順を用意していたが，通常時に比べて厳格すぎる手順を用意しており，かえって復旧が滞ってしまったという事例もあった．

復旧にかかる時間も事故の頻度も他の 3 グループと比較するとさほど多くはないが，全ての要因の中では中程度の頻度がある要因である．こういった予測不足のトラブルこそ，事例として収集し周知することで予測することができるようになるのではないかと考えられる．

5.1.4 ④事故の頻度はさほど多くないが，復旧に時間がかかる要因グループ

グループ④に含まれている要因は 4 つあり，要因番号 12「現状分析が不足していた」, 16「開

発を遂行するために必要な要員，予算，設備，期間などを確保できていなかった」，20「要求されるシステム性能を満たすために容量・能力に関する要求事項を特定し，また将来必要とされる容量・能力も予測する」，75「システムに脆弱性を残していた」である．

グループ④の共通点は，システム開発へ投入すべきリソースの不足に関わる要因が多いことである．要因番号 12,16,20 は開発やシステムに必要とされるものが不足していた要因である．要因番号 12 と 16 は現状分析の不足，要員の不足，スケジュールの短さからシステムが完成しなかったり障害が発生したりして，稼働予定日が大幅に遅れる事例が多かった．要因番号 20 はシステムの性能が不足していたという要因であり，新規オープンなどで予想外のアクセス量があったため処理能力不足に陥りシステムが利用できなくなる事例が多かった．処理能力不足を補うためのシステムの増強に時間がかかり，復旧までに時間がかかった．

要因番号 75 は OS の修正ファイルを適用しなかったなど，セキュリティ運用の初歩的なミスをした事例が多数を占め，システムの脆弱性を突かれて個人情報が盗まれるなど重要な事態となることが多かった．従って，万全なセキュリティ体制を整えて運用を再開させなければいけないため，復旧に時間がかかっている．

この 4 つの要因のうち 3 つは運用フェーズ前の要因であり，もう 1 つはセキュリティに関する要因である．このグループ④と同じく復旧に時間がかかる要因グループであるグループ①に含まれる要因番号 7 も運用フェーズ前の要因であり，運用フェーズより前の要因は復旧時間にかなりの時間がかかりやすい傾向にあるのではないかと考えられる．

5.2 要件定義の専門家による評価

第 3 節で述べた分析結果および第 4 節で述べた要件定義支援環境の提案について，IPA の TRM 推進委員会（平成 26 年度）においてレビューしていただき，コメントをいただいた．TRM 推進委員会（主査：本田実（城西国際大学））は，TRM の拡充・普及のために設けられた委員会であり，中央省庁の CIO 補佐官を中心に，自治体情報システムの管理者，情報ベンダーのプロジェクトマネージャー，学術経験者など要件定義の専門家から構成されている．

5.2.1 事故事例の要因項目に基づく分析についての評価

●事故事例の収集について

情報システムの事故やその要因については，システムを保持する企業や開発担当ベンダーからその全貌が公表されることが少ない．その意味で 30 年以上にわたる「動かないコンピュータ」の連載記事は，信頼を得ている専門誌における取材に基づいた記事であることからも，我が国の情報システムの問題を幅広く捉えた貴重な資料と言える．この資料を要件定義の場面において参照しやすい形にまとめたことは大いに意義があると，まず研究の着眼点に関して評価を得た．しかしながら，取材する事故の選択，取材内容とその分析・考察などに関しては，記者や編集者の主観による部分も含まれていると考えられるので，あくまで参考資料として参照されるように注意して提供する必要があることが指摘された．

事故の要因が述べられていない場合には，個人的に推測することや関係者にヒアリングを行うなど要因を求める手段が個々に存在する．しかし，分析の均一性を保つには，本研究のように要因が述べられていない記事は除去するのが妥当であろう．情報システム開発のそれ自身の過程ではなく，外部要因が事故を引き起こす根本原因であることは少なくない．外部要因の追求や対策は内部要因のそれらとは異種のもので，この研究において対象外としていることは頷けるが，今後の課題として欲しいといった指摘を受けた．

●事故事例の要因分類について

収集した事故事例を要因ごとに分類する作業は，本研究において各要因の重要度を求めるために最も大切な作業であり，難しい作業でもある．システム管理基準および情報セキュリティ基準に基づいて事故事例 270 件を要因ごとに分類しているが，この 2 つの基準は情報システムの開発プロセスに関して網羅性が高く妥当な方法と考えられる．またこれらの基準は，我が国における情報システム開発の注意点をまとめたものとして省庁や企業においても比較的知られているものであるので，要件定義の担当者にも分類の考え方を理解させる上で有利であるとの評価を得た．個々の事故事例の要因項目への分類の正確さについては，委員のなかの実務経験が豊富な専門家に詳しく見ていただいたが，その正確さについて要因の重要度分析に影響を与えるような大きなミスはないという評価を得た．

●要因分類に基づく事故の傾向分析について

グループ①の要因番号 7「開発計画は，目的，対象業務，費用，スケジュール，開発体制，投資効果などを明確にしなかった」が最も頻度が高く，かつ事故の被害が大きいというのは状況認識と直観的に合致するし，もっとも回避したい事故の種類と考えていることでもある．この要因に対しては，要件定義における記述も重要であるが，要件定義以前における経営者や CIO を中心とした開発体制の整備に拠るところが大きいかもしれない．今後の課題として欲しいといった指摘を受けた．

グループ④の要因番号 12「現状分析が不足していた」，16「開発を遂行するために必要な要員，予算，設備，期間などを確保できていなかった」，20「要求されるシステム性能を満たすために容量･能力に関する要求事項を特定し，また将来必要とされる容量・能力も予測する」，75「システムに脆弱性を残していた」は，まさに手を抜けば痛い目に合う項目であり，要件定義書において注意を喚起することの遣り甲斐がある項目と言える．

このほか復旧が短期であるグループ②やグループ③の要因の分析も妥当であると思うが，これらは 10 件以上事故を引き起こしている要因に限られて述べられている．10 件未満の要因のなかに重要なものはないか興味は尽きない．事故数だけでなく他の属性も合わせると今とは異なる要因がクローズアップされるのではないかという指摘も受けた．

●事故の要因項目と要件定義の要件項目の対応について

この研究では，事故を抑止するための取り組みを要件定義書作成に絞って設定しようとしている．事故の要因は，要件定義段階だけではなく，計画段階や開発段階あるいは運用段階においても作りこんでしまう危険性があるはずである．しかし，270 件の事故のうち 9 件を除いて他はすべて要件定義書の記述項目に関係付けることが可能であったことで，改めて要件定義の重要性を認識した思いである．ところが，テスト要件に目をやるとこれの重要度を少し高く評価すぎている可能性があると感じた．テストそのものはしっかりとやる必要があるが，テスト要件そのものが問題となるケースはあまりなく，むしろテストの実行そのものに問題が生じさせるケースが多いことが指摘された．要件定義フェーズと実際のテスト工程での問題は分けて考える必要があるが，明確に分けることができていない可能性がある．事故要因が要件定義フェーズに関わるものかどうかを見直していく必要がある．

要件項目と TRM および非機能要求グレードの項目との対応が可能なことは，これらの開発の主旨からもある程度予想されたもので違和感はないという指摘を受けた．

5.2.2 要件定義支援環境について

●参考となる政府調達仕様書の収集について

要件定義を記述する際には，システムを構成する技術や業務，品質に関わる知識だけではなく，その知識をどのように書いたら良いのかという手本が必要である．実際に政府が行った調達の仕様書が手本となり得るが，要件定義支援環境の利用者が要件を定義しようとしているシステムと手本のシステムに大きな差異がある場合，利用者は応用方法を考えながら参照しなくてはならない．そのため，様々なタイプの調達仕様書を収集し掲載することに大きな意義がある．現在様々なタイプの調達仕様書を収集したサイトは存在しておらず有用な機能と言えるという指摘を受けた．

●想定する利用者とニーズへの対応について

この支援環境の第一の利用者は，経験の少ない要件定義担当者である．要件定義書のテンプレートと要件定義を記述する上で参考となる事故事例，事故要因，要件定義記述のための参考資料などをコンパクトに関連付けて掲載していることは，経験の少ない担当者が短期間に知識を得る上で有益であると評価を受けた．しかし，これらのコンテンツには，読むために必要とする知識のレベルや，書式の親しみやすさのレベルの異なるものが多く，多くの読者を得るかという点ではコンテンツの洗練度アップに課題を残しているという指摘を受けた．

この支援環境の第二の利用者は，要件定義の方法やそれに関連する知識を学習しようとする若手の技術者や学生である．これら第二の利用者に対しては，情報システムの役割や要件定義記述の重要性に対する認識を深めるという観点で，事故事例記事の紹介が特に有効と考えられる．なかでも学生を対象とする場合については，レビューしていただいた専門家たちよりも大学に籍を置く報告者らが強く感じていることであるが，事故事例やその要因に関する分析と解説コンテンツの制作を強化し，情報システムや要件定義に関して興味を持ち発展的に学習するきっかけを与えることが重要と考えられる．一方，しっかりと知識を獲得してもらうためには，第二の利用者は参考資料や事故事例紹介に現れる情報システムの構成要素や動作に関しての基礎技術知識が少ないので，それらをやさしく解説するコンテンツも補う必要となることが指摘された．

6 結論

6.1 結論

本研究では，381 件の情報システムの事故事例を収集し，事故の要因ごとに分類を行って，被害の大きさや頻度に基づいて事故要因の傾向を分析した．もっとも重大な要因として「開発計画が不明確」という要因があげられたことや，情報システム開発上の要因がわかっている 270 件のうちの 261 件については要件定義項目との関連を持つことなどの分析結果や，事例収集～要因分類～分析～要件定義との関係付けの過程について CIO 補佐官などの専門家のレビューを受けた．すると，彼らが開発現場において直観的に感じていることと分析結果がおおむね合致することや，事例収集～要因分類～分析～要件定義との関係付けの過程についても，標準化モデルを基にしているは妥当であることなど評価を得た．一方，本研究では対象外とした，記事の上で要因が解明されていない事故や，情報システム開発の外部要因による事故に関しても見逃せない問題であることなどの指摘を受けた．

さらに上記の分析結果を用いて，要件定義書のひな型と，要件定義の各項目と関係する事故事例，事故要因，要件定義に参考となる資料や事例を関連付けて提供する要件定義支援環境を設計した．これも専門家のレビューを受けたところ，関係する情報がコンパクトに提供されるので，経験の少ない要件定義担当者に適しているという評価を得た．一方，多くの利用者に参照されるためには，コンテンツの充実と洗練が課題であると指摘された．

6.2 今後の課題

今後の課題として，3つの課題が挙げられる．

まず1つは，提案した要件定義支援環境の実用化に向けて試作評価のステージを進めることである．現在は，部分的な試作によって利用者の動作と表示される情報の骨格を実現し，専門家による定性的な評価を得た段階である（第一ステージ）．これを，限定した利用者において要件定義を実施できるレベルまで試作の範囲と品質を高めて利用者に提供し，実際のシステム構築での利用に供するための具体的な課題を抽出するステージ（第2ステージ）に進めたい．たとえば，著者らが所属する静岡大学大学院情報学研究科（平成27年度では総合科学技術研究科情報学専攻と改名している）では，学生自身が考えた情報システムの提案を行い，その要件定義書を作成する情報システム設計論という講義を開講している．本研究で提案した要件定義支援環境をこのような講義で使用し，学生から評価を取ることが考えられる．こうした教育の場などでの利用評価を踏まえて，省庁や企業における要件定義での利用のステージ（第3ステージ）に進みたい．第3ステージにおいては，学習者の知識獲得や情報システム開発のリスク低減を定量的に計測したいと考えている．

要因項目と要件項目の対応付けにも課題が残っている．今回の専門家による評価では，大きなミスはないという評価を得ているが，本来の狙いは，必要な要件項目の記述の品質を向上させて，開発から運用にかけてのフェーズにおいて事故要因が発生することを抑止することにある．そのためには，提供した参考情報の内容と要件定義担当者の理解の一致，要件定義担当者による要件の記述と開発ベンダーのプロジェクトマネージャーの理解の一致，さらにプロジェクトマネージャーの施策の指示と開発・運用担当者の理解・実行の一致を実質的に確保するという観点で適切な対応付けが必要である．専門家とのレビューを重ねるほか，実際的な利用のなかでステークホルダ間の情報や意思の伝達を評価し，適した対応付けを求めていきたい．

最後に事故事例の拡充と品質向上があげられる．本研究では日経コンピュータの事故事例記事を用いたが，編集者によって記事の書き方に差異があり，記事によっては事故の要因が得られなかったものもあって要因分析ができたのは270事例に留まった．個々の事例に関して追加の取材を行えば一つ一つの分析の精度は高まるだろうが，それを全体の事例に展開するのは負荷が大きい．出版された記事をもとにした分析には限界があるので，さらに多くの事例に対して要因分析を行うためには，全国の開発現場や運用現場に対して効率的にアンケートを取る方法，もしくは定形のレポートを受け付ける方法などと事故事例に基づく情報サービスを結び付けていく必要があると考えている．

謝辞

本研究の分析方法，分析結果および支援環境の提案に対しレビューをしていただいた，IPAのTRM推進委員会（平成26年度）の委員の皆様に感謝いたします．

参考文献

[1] 各府省情報化統括管理者(CIO)連絡会議決定：「情報システムに係る政府調達の基本方針」，(2007-3) 入手先 <http://www.soumu.go.jp/main_content/000070266.pdf>

[2] 経済産業省商務情報政策局情報処理振興課，独立行政法人情報処理推進機構：「情報システム調達のための技術参照モデル(TRM)物品調達編 - 平成25年度版」，(2013)，入手先 <http://www.ipa.go.jp/files/000042478.pdf>

[3] 経済産業省商務情報政策局情報処理振興課，独立行政法人情報処理推進機構：「情報システム調達のための技術参照モデル(TRM)役務調達編 - 平成25年度版」，(2013)，入手先 <http://www.ipa.go.jp/files/000042443.pdf>

[4] 独立行政法人情報処理推進機構ソフトウェア・エンジニアリング・センター:「非機能要求グレード」, (2013.4), 入手先 http://www.ipa.go.jp/sec/softwareengineering/reports/20100416.html

[5] 情報処理推進機構:「共通フレーム2013」,(2013-3)

[6] ISO/IEC/IEEE 15288:2015 (JIS X 0170:2013) システムライフサイクルモデル

[7] 総務省行政管理局:「情報システムに係る政府調達の基本指針」実務手引き, (2007.7.1), 入手先 <http://www.soumu.go.jp/main_content/000141665.pdf>

[8] 日経 BP 社:「動かないコンピュータ」,『日経コンピュータ』(2001.1.1-2014.9.24)

[9] 経済産業省:「システム管理基準」, (2004.10), 入手先 <http://www.meti.go.jp/policy/netsecurity/downloadfiles/system_kanri.pdf>

[10] 経済産業省:「情報セキュリティ管理基準(平成 20 年改正版)」, (2008), 入手先 <http://www.meti.go.jp/policy/netsecurity/downloadfiles/IS_Management_Standard.pdf>

[11] 湯浦克彦:「実践エンタープライズ・アーキテクチャ」, ソフトリサーチセンター刊, (2005)

[12] Chief Information Officers Council(連邦 CIO 協議会):"Federal Enterprise Architecture Framework Version 1.1", (1999) 入手先 http://www.enterprise-architecture.info/Images/Documents/Federal%20EA%20Fram ework.pdf

[13] Office of Management and Budget(アメリカ合衆国行政管理予算局):"Federal Enterprise Architecture Framework Version 2", (2013) 入手先 https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/fea_v2.pdf

[14] IT アソシエイト協議会, 経済産業省:「EA 策定ガイドライン Ver. 1.1」, (2003) 入手先 http://www.meti.go.jp/policy/it_policy/itasociate/it.associate.htm

[15] 情報処理推進機構 ソフトウェア・エンジニアリング・センター:「重要インフラ情報システムの信頼性向上の取り組みガイドブック」, (2011.1). 入手先 http://www.ipa.go.jp/files/000004556.pdf

[16] 遠藤正之, 高野研一:「金融事業経営における情報システム開発のリスクマネジメント観点の提案」,『日本情報経営学会誌』, Vol.33,No.3, (2013)

[17] 宮坂美樹, 山本秀男:「IT システム統合プログラムのリーダーシップに関する考察」, 国際プロジェクトマネジメント学会ジャーナル, Vol.5 No.1, pp.103-115, (2010)

[18] 西岡茂樹:「企業合併に伴う情報システム統合のリスクに関する考察」, 日本情報経営学会誌, Vol.34 No.1, pp.52-63 (2013)

[19] 坂東幸一, 田中健次:「金融情報システム事故に関する新聞報道の分析と評価」, 信頼性工学, Vol.31, No.1, (2009)

[20] 坂東幸一, 田中健次:「新聞報道による情報システム事故の信頼性・安全性の分析」, 信頼性工学, Vol.31, No.6, (2009)

[21] 日本銀行金融機構局:「事例から見たコンピュータ・システム・リスク管理の具体策」, BOJ Reports & Research Papers, (2007-03) 入手先 https://www.boj.or.jp/research/brp/ron_2007/data/ron0703a.pdf

[22] 青山幹雄, 中谷多哉子, 鈴木律郎:「要求工学知識体系 (REBOK) の誕生」, 情報処理学会デジタルプラクティス 4(2), 96-104, (2013-04)

[23] 齊藤康廣, 門田暁人, 松本健一:「非機能要件に着目した Request For Proposal(RFP) 評価」, SECjournal, Vol.10 No.3, pp.30-37 (2014-09)

[24] 佐藤知徳, 他 5:「ソフトウェア要求仕様書における品質要求の含有率測定ツールの設計」, 信学技法 KBSE2007-57 (2008-03)

[25] ISO/IEC 9126-1:2001 Software Engineering
[26] 経済産業省 :「情報システム調達のための技術参照モデル (TRM) システム開発調達仕様書 < ひな形 >- 平成 25 年度版 (H26.10)」, (2014), 入手先 <http://www.ipa.go.jp/osc/trm/>
[27] 経済産業省 :「情報システム調達のための技術参照モデル (TRM) 運用管理支援調達仕様書 < ひな形 >- 平成 25 年度版 (H26.10)」, (2014), 入手先 <http://www.ipa.go.jp/osc/trm/>
[28] 経済産業省 :「情報システム調達のための技術参照モデル (TRM) 機器賃貸借及び保守調達仕様書 < ひな形 >- 平成 25 年度版 (H26.10)」, (2014), 入手先 http://www.ipa.go.jp/osc/trm/
[29] 厚生労働省政策統括官付情報政策担当参事官室 :「医療保険者等向け中間サーバー等ソフトウェア設計・開発等業務 調達仕様書 (案)」, (2014.11), 入手先 <http://www.mhlw.go.jp/sinsei/chotatu/chotatu/shiyousho-an/dl/141126-1.pdf>
[30] 厚生労働省医薬食品局安全部監視安全課中毒被害情報管理室 :「食品保険総合情報処理システム システム更改・運用保守業務一式仕様書」, (2015.1) , 入手先 <http://www.mhlw.go.jp/sinsei/chotatu/chotatu/shiyousho-an/dl/150130-2_01.pdf>